LEÇONS

SUR LA

RÉSOLUTION ALGÉBRIQUE

DES ÉQUATIONS

LEÇONS

SUR LA

RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS

PAR

H. VOGT

ANCIEN ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE,
PROFESSEUR ADJOINT A LA FACULTÉ DES SCIENCES DE NANCY

Avec une Préface

DE

M. JULES TANNERY

DIRECTEUR DES ÉTUDES SCIENTIFIQUES A L'ÉCOLE NORMALE SUPÉRIEURE

PARIS

VUIBERT ET NONY, ÉDITEURS

63, Boulevard Saint-Germain, 63

PRÉFACE

En me demandant d'écrire quelques mots en tête du présent livre, M. Vogt a montré une modestie qui est peut-être excessive et m'a donné un témoignage d'affection qui, à coup sûr, m'est très précieux. Ce livre, à ce que je crois, n'avait nul besoin d'être recommandé : le grand intérêt du sujet qu'il traite, la clarté avec laquelle il est écrit, suffisaient à le faire bien accueillir des lecteurs. Pour quelques-uns, sa brièveté même sera un mérite : quelque désir qu'on ait d'acquérir des connaissances nouvelles, dont on sent l'importance, on est parfois découragé par l'effort qu'elles semblent exiger, par le temps qu'il y faudrait consacrer, et qui manque. Un petit livre est rassurant.

Celui-ci est plein de choses et des plus belles. Je ne sais s'il existe en mathématiques un sujet qui ait exigé de ceux qui l'ont traité plus d'ingéniosité, plus de profondeur et de

pénétration que n'a fait cette théorie des équations algébriques, dont Lagrange, Gauss, Abel et Galois ont été les fondateurs. A la vérité, la beauté de leur œuvre est si merveilleuse qu'elle risque parfois d'éloigner d'elle quelques jeunes mathématiciens, trop modestes pour prétendre la continuer, ou trop pressés d'aller chercher ailleurs une moisson plus facile. Est-ce une raison pour ne pas l'étudier, si même cette étude devait se borner à une pure contemplation, et comme à une jouissance esthétique? Je ne veux pas parler ici des prolongements extraordinaires que la pensée des grands géomètres que je viens de nommer, d'Évariste Galois en particulier, s'est trouvée avoir dans d'autres directions, mais, en restant dans les éléments, est-il possible que ceux qui ont étudié le cours d'algèbre de notre classe de mathématiques spéciales ne sentent pas leur curiosité s'éveiller devant les problèmes qui se posent là d'une façon nécessaire, est-il possible qu'ils ne soupçonnent pas que, pour bien des sujets qu'ils ne font qu'effleurer, la vraie lumière est plus loin, dans un domaine où ils n'ont pas le temps de pénétrer? Ne faut-il pas, autant qu'il est possible, indiquer à ceux dont la curiosité est trop vive et trop pressée de quel côté est ce domaine, et en faciliter l'accès à ceux qui, débarrassés du souci des examens, ont gardé le goût de la science et conquis la liberté d'étudier ce qui les intéresse? C'est pour ceux qui se destinent à l'enseignement que cette étude de l'Algèbre est le plus nécessaire : elle est vraiment

indispensable à ceux qui doivent parler un jour des fonctions symétriques, de la transformation des équations, de la résolution des équations du troisième et du quatrième degré, des équations de la division du cercle. Sans doute, ils n'auront à traiter ni des substitutions, ni du groupe de Galois, ni des équations abéliennes ; mais, s'ils possèdent ces théories, les sujets élémentaires qu'ils ont à développer leur apparaîtront dans leur véritable jour, dans leur véritable importance, dans leur sens profond ; les exemples intéressants se présenteront en foule à leur esprit, et, parfois, sur quelqu'un de ces exemples, sur un fait précis et particulier, ils sauront faire soupçonner à leurs élèves les théories qu'ils n'ont pas le loisir d'aborder. Montrer que la science n'est pas bornée à ce qu'il enseigne immédiatement, qu'elle ne se réduit pas à des artifices qui permettent de traiter des problèmes fabriqués exprès pour les utiliser, faire pressentir la grandeur de la science et, ainsi, en inspirer le respect, c'est, pour le maître, la partie vraiment noble et élevée de son métier.

Les lecteurs auxquels s'adresse M. Vogt sont donc nombreux. Sans doute, son livre n'est pas le premier qu'on ait écrit sur la matière ; sans parler des mémoires originaux, auxquels il faudra toujours recourir, mais qu'il vaut mieux étudier après avoir acquis des vues d'ensemble sur l'état actuel de la science, il est certain que le Traité d'algèbre supérieure de J. A. Serret rendra, pendant longtemps encore, de grands services ; mais, depuis le temps où il a

paru, bien des recherches importantes ont été faites, dont les résultats et l'esprit n'ont pu pénétrer dans un livre qui les avait précédées ; le Traité des substitutions de M. Jordan est une œuvre magistrale, qui s'adresse plutôt à ceux qui veulent approfondir la science qu'à ceux qui veulent s'y initier. La Théorie des substitutions de M. Netto, le Manuel d'algèbre de M. Weber, dont le premier volume vient de paraître, sont d'excellents livres, mais qui ne sont pas écrits en français. Le livre de M. Vogt vient ainsi prendre une place qui était vide, et qu'on sentait vide. Je suis persuadé que le plaisir que j'ai trouvé à le lire sera partagé par tous ceux qui l'étudieront.

Paris, le 23 Juin 1895.

JULES TANNERY.

LEÇONS

SUR LA

RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS

CHAPITRE I

DES GROUPES DE SUBSTITUTIONS

---

1. Une substitution est l'opération qui consiste à remplacer un ou plusieurs éléments par un même nombre d'autres qui leur correspondent respectivement d'après une loi déterminée. Lorsqu'on remplace par exemple une variable x par

$$\frac{ax+b}{cx+d},$$

où a, b, c, d sont des constantes, on dit que l'on effectue sur cette variable une substitution linéaire ; de même, lorsqu'on remplace deux variables x et y respectivement par $ax+by$, $cx+dy$, on effectue sur ces variables une substitution linéaire homogène ; a, b, c, d sont appelés les coefficients de la substitution.

Nous nous occuperons spécialement des substitutions suivantes :

Considérons n éléments représentés par les lettres $x_1, x_2, \ldots, x_n$ et leurs permutations linéaires, en nombre $n!$; les substitutions que nous étudions sont celles qui remplacent chaque élément d'une permutation par l'élément de même rang d'une deuxième permutation, distincte ou non de la première. Comme l'ordre des éléments qui se correspondent n'intervient pas dans le résultat, on peut supposer que chaque substitution remplace les éléments

d'une permutation fixe, par exemple $x_1, x_2, \ldots, x_n$, par ceux de même rang de chacune des $n!$ permutations ; il y a donc $n!$ substitutions distinctes.

En particulier, celle qui fait correspondre une permutation à elle-même n'altère aucun élément ; on l'appelle substitution identique ou unité, ce que l'on indique par la notation $S = 1$.

Les substitutions les plus simples non identiques sont celles qui remplacent, dans une permutation, chaque élément par celui qui le suit et le dernier par le premier ; une telle substitution est appelée circulaire, et les éléments forment un cycle.

Toute substitution de n éléments est circulaire ou se décompose en substitutions circulaires. Soit en effet x_1 un élément quelconque, x_α celui par lequel il est remplacé par la substitution donnée, x_β celui qui remplace x_α, x_γ celui qui remplace x_β, etc. ; on arrive ainsi à un élément x_λ que la substitution remplace par x_1. Les éléments $x_1, x_\alpha, x_\beta, x_\gamma, \ldots, x_\lambda$ sont permutés circulairement et forment un cycle ; dans le cas particulier où x_1 reste inaltéré par la substitution, on peut dire que cet élément forme à lui seul un cycle.

Si le premier cycle ainsi obtenu renferme les n éléments, la substitution donnée est circulaire ; dans le cas contraire, un élément x_μ n'entrant pas dans ce premier cycle donne naissance à un deuxième de la même manière, et ainsi de suite. De cette façon les n éléments sont partagés en cycles distincts n'ayant aucun élément commun, et la substitution donnée est décomposée en autant de substitutions circulaires qu'il y a de cycles ; l'ordre dans lequel sont effectuées ces substitutions partielles est indifférent.

Les substitutions circulaires dont les cycles renferment deux éléments seulement s'appellent transpositions ; une substitution circulaire quelconque se ramène à une suite de transpositions ; par exemple celle dont le cycle est $x_1 x_\alpha x_\beta \ldots x_\lambda$ se ramène à la suite des transpositions de cycles respectifs $x_1 x_\alpha, x_1 x_\beta, \ldots, x_1 x_\lambda$ effectuées dans cet ordre. Il résulte de ce qui précède que toute substitution peut être décomposée en transpositions successives.

2. On indique une substitution de différentes manières :

1° On écrit l'une au-dessous de l'autre, dans une même parenthèse, la permutation primitive et celle qui lui correspond ; exemple :

$$S = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_6 & x_4 & x_1 & x_5 & x_2 \end{pmatrix}$$

est la substitution qui remplace x_1 par x_3, x_2 par x_6, etc. ;

2° On indique une substitution circulaire de plusieurs éléments par la suite de ces éléments placés dans une parenthèse ; pour une substitution quelconque, on décompose la totalité des éléments en cycles distincts ne renfermant aucun élément commun, et l'on écrit les substitutions circulaires relatives à ces cycles à la suite l'une de l'autre, dans un ordre quelconque ; il est inutile d'écrire les éléments non altérés ; la substitution précédente s'écrira de cette façon :

$$S = (x_1x_3x_4)(x_2x_6) = (x_2x_6)(x_1x_3x_4) ;$$

3° Dans certains cas, on indique la loi qui détermine l'indice d'un élément de la nouvelle permutation en fonction de celui de l'élément correspondant de la permutation primitive ; par exemple la substitution circulaire

$$S = (x_0x_1x_2x_3)$$

sera indiquée par

$$i' \equiv i + 1 \qquad \text{(mod. 4)},$$

i et i' étant les indices de deux éléments correspondants.

3. Si l'on effectue sur un ensemble d'éléments E une substitution S le remplaçant par l'ensemble E′, puis sur E′ une substitution S′ le remplaçant par E″, la substitution S″ qui remplace E par E″ est appelée le produit de S par S′, ce que l'on indique par la notation $S'' = S.S'$; de même si l'on effectue successivement les substitutions $S_1, S_2, \dots, S_p$, le résultat peut être obtenu par une substitution S qui est appelée le produit des précédentes, ce que l'on indique par $S = S_1S_2\dots S_p$, en plaçant les facteurs dans l'ordre successif des substitutions, de gauche à droite ; le produit dépend de l'ordre des facteurs ; par exemple pour trois éléments x_1, x_2, x_3, les substitutions

$$S = (x_1x_2), \qquad S' = (x_2x_3)$$

ont pour produits

$$SS' = (x_1x_3x_2), \qquad S'S = (x_1x_2x_3).$$

On appelle substitution inverse d'une substitution S′, ce que l'on indique par la notation S^{-1}, celle qui est définie par l'une ou l'autre des égalités suivantes, qui sont équivalentes :

$$SS^{-1} = 1, \qquad S^{-1}S = 1.$$

On l'obtient en renversant dans chaque cycle l'ordre des éléments qui le composent. On écrit de plus $S.S = S^2$ et en général $S^p.S^q = S^{p+q}$ pour toute valeur positive ou négative de p et de q.

Étant donné un ensemble de substitutions distinctes

$$1, \ S_1, \ S_2, \ \ldots,$$

on dit qu'elles forment un groupe si leurs inverses, leurs puissances et leurs produits font partie du même ensemble ; on appelle ordre du groupe le nombre des substitutions qui le composent, y compris la substitution unité ; on appelle degré le nombre des éléments qui sont soumis à ces substitutions.

Pour définir un groupe, il suffit de donner une ou plusieurs substitutions fondamentales dont les puissances positives ou négatives et les produits constitueront les substitutions du groupe ; ces puissances et ces produits forment un nombre limité de substitutions distinctes, au plus égal à n ! dans le cas de n éléments ; on reconnaît que les substitutions sont fondamentales si chacune d'elles ne fait pas partie du groupe défini par les autres.

Je vais montrer qu'une seule substitution définit, par ses puissances, un groupe dont l'ordre, appelé aussi l'ordre de la substitution, est égal à l'exposant de la première puissance de cette substitution qui se réduise à l'unité.

Soit S une substitution, m le plus petit exposant tel que $S^m = 1$; les substitutions

$$S, \ S^2, \ S^3, \ \ldots, \ S^m$$

forment un groupe ; en effet : on a d'abord $S^{-1} = S^{m-1}$, car les produits de ces deux substitutions par S sont égaux à l'unité ; de plus, si p est une puissance quelconque positive ou négative, et p' un nombre positif ou nul inférieur à m tel que

$$p = mq + p',$$

on a

$$S^p = S^{mq+p'} = (S^m)^q.S^{p'} = S^{p'}.$$

Comme $S^{p'}$ est une des m substitutions considérées, on voit que les inverses, les puissances et les produits des substitutions de l'ensemble font partie de cet ensemble.

Les substitutions précédentes sont enfin distinctes, car si pour p et q égaux ou inférieurs à m et différents on avait $S^p = S^q$,

on aurait $S^{p-q} = 1$, ce qui est impossible ; on conclut de là que l'ordre du groupe est bien égal à m.

Par exemple une substitution circulaire a un ordre égal à son degré.

Une substitution quelconque se ramène, comme on l'a vu, à des substitutions circulaires relatives à des cycles n'ayant aucun élément commun, et effectuées dans un ordre quelconque ; un raisonnement immédiat montre que l'ordre de la substitution est égal au plus petit commun multiple des ordres des substitutions circulaires dont elle est composée.

Il est évident d'après cela que l'ordre d'une substitution composée de cycles de $\alpha, \beta, \ldots$ éléments, où $\alpha + \beta + \ldots \leqslant n$, est toujours inférieur à $n\,!$, et à $\frac{1}{2} n\,!$ si $n > 3$, car le plus petit commun multiple des nombres $\alpha, \beta, \ldots$ est au plus égal à leur produit, et est inférieur au produit $1, 2, \ldots, n$ et à la moitié de ce produit.

4. L'ensemble des $n\,!$ substitutions que l'on peut effectuer sur n éléments forme un groupe, car les puissances et les produits de ces substitutions font partie du même ensemble ; ce groupe est appelé le groupe symétrique des n éléments, parce que ses substitutions laissent invariable toute fonction symétrique de ces éléments.

Théorème. — *Le groupe dérivé des* $n - 1$ *transpositions*

$$(x_1x_2),\ (x_1x_3),\ \ldots,\ (x_1x_n)$$

est identique au groupe symétrique des n éléments $x_1, x_2, \ldots, x_n$.

Car d'après l'égalité

$$(x_\alpha x_\beta) = (x_1x_\alpha)(x_1x_\beta)(x_1x_\alpha),$$

une transposition quelconque est dérivée des précédentes, et il en est de même de toute substitution qui se ramène, comme on l'a vu, à une suite de transpositions. Le groupe renferme donc les $n\,!$ substitutions du groupe symétrique et lui est identique.

5. Le groupe le plus important après le groupe symétrique est le groupe alterné, formé par la substitution unité et les substitutions composées d'un nombre pair de transpositions ; il est ainsi appelé parce que ses substitutions laissent invariable la fonction

$$\Pi(x_i - x_j), \qquad i > j, \qquad i, j = 1, 2, \ldots, n$$

qui a deux valeurs égales et de signes contraires lorsqu'on effectue toutes les substitutions possibles sur les éléments $x_1, x_2, \ldots, x_n$.

Pour décomposer une substitution en transpositions, il suffit de remarquer, comme on l'a vu, qu'une substitution circulaire de p éléments, telle que $(x_1x_2\ldots x_p)$, est le produit des $p-1$ transpositions

$$(x_1x_2)(x_1x_3)\ldots(x_1x_p);$$

une substitution quelconque altérant m éléments, et composée de k cycles, est par suite le produit de $m-k$ transpositions.

Pour montrer que les substitutions composées d'un nombre pair de transpositions forment un groupe, nous nous appuierons sur le théorème suivant :

Théorème. — *Si une substitution* S *est le produit de* q *transpositions, et si on la multiplie par une transposition* T, *on forme une substitution* ST *qui renferme* $q+1$ *ou* $q-1$ *transpositions.*

Soit une substitution S portant sur m éléments et renfermant k cycles ; on a $q = m - k$; différents cas peuvent se présenter pour la transposition T :

1° Les éléments permutés par T sont distincts des m éléments altérés par S ; alors ST comprend deux éléments de plus et un cycle de plus que S, donc $q+1$ transpositions ;

2° Un des éléments de T appartient à un des cycles de S ; soit par exemple

$$S = (x_1x_2x_3x_5)(x_4x_6), \qquad T = (x_2x_7);$$

alors

$$ST = (x_1x_7x_2x_3x_5)(x_4x_6);$$

le produit ST renferme autant de cycles et un élément de plus que la substitution S, donc $q+1$ transpositions ;

3° Les deux éléments de T appartiennent à deux cycles différents de S ; soit, par exemple, dans le cas précédent, $T = (x_2x_4)$; alors

$$ST = (x_1x_4x_6x_2x_3x_5);$$

le produit renferme un cycle de moins, donc encore $q+1$ transpositions ;

4° Enfin, si les deux éléments de T appartiennent à un même cycle de S, par exemple si $T = (x_2x_5)$, on a

$$ST = (x_1x_5)(x_2x_3)(x_4x_6);$$

il y a un cycle de plus, et par suite $q-1$ transpositions, ce qui démontre le théorème.

Ceci nous montre que quelle que soit la manière de décomposer une substitution en un produit de transpositions, le nombre de ces transpositions conserve la même parité. En outre, le produit de deux substitutions d'un nombre pair de transpositions est une substitution de même nature, ce qui démontre l'existence du groupe que nous avons appelé alterné.

Théorème. — *L'ordre du groupe alterné est égal à* $\frac{n!}{2}$·

Partageons l'ensemble des $n!$ substitutions en deux parties : 1° celles qui renferment un nombre pair de transpositions, y compris l'unité, et qui composent le groupe alterné ; 2° celles qui renferment un nombre impair de transpositions et ne forment pas de groupe ; si nous multiplions les premières par une transposition quelconque T, nous formons des substitutions distinctes, faisant partie du deuxième ensemble ; de même les produits des substitutions du deuxième ensemble par une transposition quelconque sont distincts et font partie du premier ; les deux ensembles contiennent par suite le même nombre de substitutions, c'est-à-dire $\frac{1}{2}n!$

Théorème. — *Le groupe alterné contient toutes les substitutions circulaires renfermant un nombre impair d'éléments et ne contient aucune des autres.*

En effet, une substitution circulaire de p éléments est le produit de $p-1$ transpositions.

Corollaire. — *Le groupe dérivé des* $n-2$ *substitutions circulaires*

$$(x_1x_2x_3),\quad (x_1x_2x_4),\quad \ldots,\quad (x_1x_2x_n)$$

est le groupe alterné des n *éléments* x_1, x_2, $\ldots$, x_n.

En effet, toute substitution circulaire de trois éléments est un produit des précédentes, d'après l'égalité

$$(x_\alpha x_\beta x_\gamma) = (x_1x_2x_\alpha)(x_1x_2x_\gamma)(x_1x_2x_\beta)(x_1x_2x_\alpha)(x_1x_2x_\alpha)(x_1x_2x_\gamma)$$
$$(x_1x_2x_\alpha)(x_1x_2x_\gamma)(x_1x_2x_\gamma).$$

De plus, le produit de deux transpositions est un produit des substitutions précédentes, car

$$(x_\alpha x_\beta)(x_\alpha x_\gamma) = (x_\alpha x_\beta x_\gamma),$$
$$(x_\alpha x_\beta)(x_\gamma x_\delta) = (x_\alpha x_\beta x_\gamma)(x_\alpha x_\delta x_\gamma);$$

le groupe renferme ainsi tous les produits d'un nombre pair de transpositions ; par suite, il est identique au groupe alterné.

On conclut de là qu'un groupe renfermant toutes les substitutions circulaires d'ordre 3 se confond avec le groupe alterné ou avec le groupe symétrique. En effet, il renferme d'abord toutes les substitutions du groupe alterné, comme on vient de le voir, par suite toutes celles qui sont composées d'un nombre pair de transpositions ; s'il en renferme une autre, composée d'un nombre impair de transpositions, il contient les produits par cette dernière des substitutions du groupe alterné, et ces produits constituent, avec celles-ci, toutes les substitutions du groupe symétrique.

On verrait de la même manière qu'un groupe contenant toutes les substitutions circulaires d'ordre 5 se confond avec le groupe alterné ou bien avec le groupe symétrique, car on a

$$(x_\alpha x_\beta x_\gamma) = (x_\alpha x_\gamma x_\varepsilon x_\beta x_\delta)(x_\alpha x_\delta x_\gamma x_\beta x_\varepsilon) ;$$

par suite le groupe contient toutes les substitutions circulaires du troisième ordre et celles du groupe alterné ; il se confond avec lui ou avec le groupe symétrique.

CHAPITRE II

DES SOUS-GROUPES. — GROUPES SIMPLES ET COMPOSÉS

---

6. On dit qu'un groupe G contient un autre groupe G' s'il renferme toutes les substitutions de cet autre ; le second groupe G' est appelé sous-groupe du premier.

Théorème. — *L'ordre d'un sous-groupe d'un groupe donné est un diviseur de l'ordre de ce groupe.*

Soit un groupe G et un sous-groupe G' composé des substitutions

(1) $$S_1 = 1, \quad S_2, \quad S_3, \quad \ldots, \quad S_{r'}.$$

Si Σ_2 est une substitution du groupe G non contenue dans G', les substitutions

(2) $$S_1\Sigma_2, \quad S_2\Sigma_2, \quad \ldots, \quad S_{r'}\Sigma_2$$

jouissent des propriétés suivantes :

1° Elles sont distinctes l'une de l'autre, car si l'on avait par exemple $S_\alpha\Sigma_2 = S_\beta\Sigma_2$, les produits de ces substitutions par Σ_2^{-1}, qui sont respectivement S_α et S_β, seraient égaux, ce que nous ne supposons pas ;

2° Elles sont distinctes des précédentes, car si $S_\alpha\Sigma_2$ était égal à S_β, on aurait $\Sigma_2 = S_\alpha^{-1}S_\beta$, et Σ_2 ferait partie du groupe G', ce qui est impossible ;

3° Elles font partie du groupe G.

S'il existe dans le groupe G d'autres substitutions que les précédentes, et si Σ_3 est une telle substitution, on verra de même que l'ensemble

(3) $$S_1\Sigma_3, \quad S_2\Sigma_3, \quad \ldots, \quad S_{r'}\Sigma_3$$

jouit des mêmes propriétés ; les substitutions qu'il renferme sont distinctes l'une de l'autre, distinctes de celles de l'ensemble (1), et aussi de celles de l'ensemble (2), car si l'on avait $S_\alpha \Sigma_3 = S_\beta \Sigma_2$, on aurait $\Sigma_3 = (S_\alpha^{-1} S_\beta)\Sigma_2$ et Σ_3 ferait partie de l'ensemble (2), ce qui est impossible ; elles font enfin partie du groupe G.

En continuant de cette façon, on voit que, si l'on représente par Σ_1 la substitution unité, on peut ranger les substitutions du groupe G en un tableau de la forme

$$(4) \qquad \left\{ \begin{array}{llll} S_1\Sigma_1, & S_2\Sigma_1, & \ldots, & S_{r'}\Sigma_1 \\ S_1\Sigma_2, & S_2\Sigma_2, & \ldots, & S_{r'}\Sigma_2 \\ \ldots & \ldots & \ldots & \ldots \\ S_1\Sigma_\rho, & S_2\Sigma_\rho, & \ldots, & S_{r'}\Sigma_\rho \end{array} \right.$$

où $\Sigma_1 = 1, \Sigma_2, \ldots, \Sigma_\rho$ sont des substitutions convenablement choisies de ce groupe ; il les renferme toutes et chacune une seule fois ; par suite l'ordre r du groupe G est égal a $r'\rho$, ce qui démontre le théorème.

Corollaire I. — *L'ordre d'un groupe est un diviseur de n!*

Car un groupe quelconque est un sous-groupe du groupe symétrique, dont l'ordre est n!

Corollaire II. — *Les substitutions communes à deux groupes forment un troisième groupe qui est contenu comme sous-groupe dans chacun des premiers.*

En effet, les inverses, les puissances et les produits des substitutions communes à deux groupes sont également communs à ces deux groupes, ce qui montre que les substitutions communes forment un groupe ; c'est un sous-groupe de chacun des premiers, et son ordre est un diviseur commun aux ordres de ces groupes.

Si ces ordres sont premiers entre eux, les deux groupes ne peuvent avoir d'autre substitution commune que la substitution unité.

7. Étant donnée une substitution S et une autre T, on appelle transformée de la première par la seconde la substitution $T^{-1}ST$.

Si l'on désigne par substitutions semblables celles qui sont composées d'un même nombre de cycles, portant respectivement sur un même nombre de lettres, deux substitutions transformées l'une de l'autre sont toujours semblables.

En effet, soit

$$S = (x_1x_2x_3\dots)(x_h\dots)\ ..$$

la substitution S décomposée en cycles, et

$$T = \begin{pmatrix} x_1x_2x_3\dots\ x_h\dots\ x_n \\ x_\alpha x_\beta x_\gamma\dots\ x_\lambda\dots\ x_\nu \end{pmatrix}$$

une autre substitution par laquelle on transforme la première ; en appliquant successivement les substitutions T^{-1}, S et T, l'élément x_α est remplacé par x_1, x_2 et x_β; la transformée $T^{-1}ST$ change par suite x_α en x_β, de même x_β en x_γ, etc. ; on voit de cette façon que l'on obtient cette transformée en remplaçant chacune des lettres de S par celle que T lui fait correspondre, de sorte que

$$T^{-1}ST = (x_\alpha x_\beta x_\gamma\dots)(x_\lambda\dots)\ \dots\ ;$$

les deux substitutions sont bien semblables.

Réciproquement, deux substitutions semblables sont transformées l'une de l'autre par une troisième substitution, celle qui remplace chaque lettre de la première par la lettre de même rang dans la seconde, en supposant que l'on ait écrit les cycles successifs de façon que ceux qui possèdent le même nombre de lettres se correspondent dans les deux substitutions.

Comme conséquence, on peut remarquer que les produits ST et TS, qui sont en général différents, sont semblables, car l'un est une transformée de l'autre d'après l'égalité

$$ST = T^{-1}(TS)T.$$

Théorème. — *Les transformées des substitutions d'un groupe* G *par une même substitution forment un groupe.*

Si l'on considère en effet deux substitutions quelconques S_1 et S_2 du groupe G et leurs transformées par T : $T^{-1}S_1T$, $T^{-1}S_2T$, leur produit

$$(T^{-1}S_1T)(T^{-1}S_2T) = T^{-1}(S_1S_2)T$$

est la transformée d'une substitution du groupe et fait partie du même ensemble que les transformées de S_1 et de S_2.

Le nouveau groupe est appelé transformé du groupe G par la substitution T, et est indiqué par la notation $T^{-1}GT$.

8. On dit que deux substitutions S et T sont permutables si les produits ST et TS sont égaux ; chacune d'elles est égale à sa trans-

formée par l'autre, car de l'égalité $ST = TS$, on déduit $T = S^{-1}TS$ et $S = T^{-1}ST$.

De la même manière on dit qu'un groupe G est permutable à une substitution T si le groupe $T^{-1}GT$ transformé de G lui est identique, à l'ordre près des substitutions, c'est-à-dire si l'on a, quel que soit α, une égalité de la forme

$$T^{-1}S_\alpha T = S_\beta;$$

les transformées des substitutions de G étant distinctes reproduisent, dans un ordre quelconque, les substitutions de ce groupe, de sorte que les ensembles $(S_\alpha T)$ et (TS_α) sont identiques à l'ordre près.

Si un groupe G est permutable à deux substitutions T et T_1, il est permutable à leur produit, car

$$(TT_1)^{-1}S_\alpha(TT_1) = T_1^{-1}T^{-1}S_\alpha TT_1 = T_1^{-1}S_\beta T_1 = S_\gamma,$$

en désignant par S_β la transformée de S_α par T, et par S_γ celle de S_β par T_1.

On conclut de là que les substitutions auxquelles un groupe est permutable forment elles-mêmes un groupe.

On dit qu'un groupe G est permutable à un groupe H s'il est permutable à toute substitution de ce groupe ; on indique cette propriété par la notation

$$H^{-1}GH = G.$$

Si un sous-groupe G_1 d'un groupe G est permutable à ce groupe, on dit que G_1 est un sous-groupe distingué ou invariant de G.

Comme exemple, le groupe alterné est un sous-groupe invariant du groupe symétrique, car la transformée d'une substitution du groupe alterné par une substitution quelconque renferme un nombre pair de transpositions et appartient au groupe alterné.

Comme autre exemple, considérons le cas de $n = 4$; le groupe symétrique contient 24 permutations et le groupe alterné 12.

Ce groupe alterné est constitué par les substitutions

$$S_1 = 1, \quad S_2 = (x_1x_2)(x_3x_4), \quad S_3 = (x_1x_3)(x_2x_4), \quad S_4 = (x_1x_4)(x_2x_3) = S_2S_3,$$

$$S_5 = (x_1x_2x_3), \qquad S_6 = (x_1x_3x_2) = S_5^2,$$

$$S_7 = (x_1x_3x_4) = S_2S_5, \qquad S_8 = (x_2x_3x_4) = S_2S_5^2,$$

$$S_9 = (x_2x_4x_3) = S_3S_5, \qquad S_{10} = (x_1x_2x_4) = S_3S_5^2,$$

$$S_{11} = (x_1x_4x_2) = S_4S_5, \qquad S_{12} = (x_1x_4x_3) = S_4S_5^2;$$

on voit qu'il dérive des substitutions S_2, S_3 et S_5, d'ordres respectifs 2, 2 et 3.

Le groupe symétrique est formé des substitutions précédentes et de leurs produits par une transposition quelconque, par exemple $T = (x_1 x_2)$; nous le représenterons par G et le groupe alterné par G'.

Le groupe d'ordre 4,

$$H = (S_1 = 1, S_2, S_3, S_4),$$

est un sous-groupe du groupe alterné ; il est permutable au groupe symétrique ; en effet : il l'est d'abord aux substitutions S_2, S_3 et S_4 du groupe H ; il l'est aussi à S_5, car

$$S_5^{-1} S_2 S_5 = S_4, \qquad S_5^{-1} S_3 S_5 = S_2, \qquad S_5^{-1} S_4 S_5 = S_3 ;$$

il l'est enfin à la transposition T, car

$$T^{-1} S_2 T = S_2, \qquad T^{-1} S_3 T = S_4, \qquad T^{-1} S_4 T = S_3 ;$$

par suite, il l'est à toute substitution dérivée de S_2, S_3, S_5 et T.

Le groupe H est donc un sous-groupe invariant du groupe symétrique, et aussi du groupe alterné.

On verrait de la même manière que chacun des groupes d'ordre 2,

$$K_1 = (S_1, \quad S_2), \qquad K_2 = (S_1, \quad S_3), \qquad K_3 = (S_1, \quad S_4),$$

est un sous-groupe invariant du groupe H, sans l'être du groupe symétrique ni du groupe alterné.

9. Soient

$$G = (S_1 = 1, \quad S_2, \quad \ldots, \quad S_r),$$
$$H = (T_1 = 1, \quad T_2, \quad \ldots, \quad T_{r'})$$

deux groupes permutables l'un à l'autre, c'est-à-dire tels que

$$H^{-1} G H = G, \qquad G^{-1} H G = H ;$$

on sait (§ 6) que les substitutions communes forment un groupe

$$K = (U_1 = 1, \quad U_2, \quad \ldots, \quad U_\rho),$$

dont l'ordre ρ divise r et r', de sorte que $r = \rho p$, $r' = \rho p'$; de plus, que l'on peut écrire les groupes G et H sous forme de tableaux comme il suit

$$G = \begin{cases} U_1\Sigma_1, & U_2\Sigma_1, & \ldots, & U_\rho\Sigma_1 \\ U_1\Sigma_2, & U_2\Sigma_2, & \ldots, & U_\rho\Sigma_2 \\ \ldots & \ldots & \ldots & \ldots \\ U_1\Sigma_p, & U_2\Sigma_p, & \ldots, & U_\rho\Sigma_p \end{cases} \qquad H = \begin{cases} U_1\Sigma'_1, & U_2\Sigma'_1, & \ldots, & U_\rho\Sigma'_1 \\ U_1\Sigma'_2, & U_2\Sigma'_2, & \ldots, & U_\rho\Sigma'_2 \\ \ldots & \ldots & \ldots & \ldots \\ U_1\Sigma'_{p'}, & U_2\Sigma'_{p'}, & \ldots, & U_\rho\Sigma'_{p'} \end{cases}$$

où Σ_α et Σ'_β sont des substitutions convenablement choisies, et où Σ_1 et Σ'_1 représentent en particulier la substitution unité. Je vais démontrer le théorème suivant :

THÉORÈME. — *Les substitutions* $U_\alpha\Sigma_\beta\Sigma'_\gamma$ *forment un groupe d'ordre* $\rho p p' = \frac{rr'}{\rho}$ *contenant les deux groupes* G *et* H *comme sous-groupes invariants, et le groupe* K *est un sous-groupe invariant à la fois de* G *et de* H.

Pour le démontrer (*), remarquons qu'un produit de la forme

$$S_\alpha T_\beta S_\alpha^{-1} T_\beta^{-1} = S_\alpha(T_\beta S_\alpha^{-1} T_\beta^{-1}) = (S_\alpha T_\beta S_\alpha^{-1}) T_\beta^{-1}$$

appartient à la fois aux deux groupes G et H, car la première et la seconde parenthèse représentent des substitutions faisant partie respectivement de ces deux groupes; il appartient par suite au groupe K. Si on le représente par U_γ, et si l'on prend son inverse $T_\beta S_\alpha T_\beta^{-1} S_\alpha^{-1}$, les égalités

$$S_\alpha T_\beta S_\alpha^{-1} T_\beta^{-1} = U_\gamma, \qquad T_\beta S_\alpha T_\beta^{-1} S_\alpha^{-1} = U_\gamma^{-1}$$

donnent, en multipliant les deux membres de la première par $T_\beta S_\alpha$, et ceux de la seconde par $S_\alpha T_\beta$,

$$S_\alpha T_\beta = U_\gamma T_\beta S_\alpha, \qquad T_\beta S_\alpha = U_\gamma^{-1} S_\alpha T_\beta.$$

En particulier, en prenant pour S_α et T_β des substitutions particulières, telles que Σ_α, Σ'_β ou bien U_α, U_β, on trouve entre les substitutions Σ, Σ' et U des relations de la forme suivante :

$$\Sigma_\alpha\Sigma'_\beta = U_\gamma\Sigma'_\beta\Sigma_\alpha, \qquad \Sigma_\alpha U_\beta = U_\delta\Sigma_\alpha, \qquad \Sigma'_\beta U_\alpha = U_\varepsilon\Sigma'_\beta.$$

Cela posé, les substitutions de la forme $U_\alpha\Sigma_\beta\Sigma'_\gamma$, où α, β, γ prennent toutes les valeurs possibles respectivement comprises entre 1 et ρ, 1 et p, 1 et p', constituent un groupe ; en effet, remarquons d'abord que l'inverse d'une substitution quelconque S est identique à la puissance de degré $m-1$ de cette substitution, m désignant son ordre ; il suffit donc de faire voir que le produit de

(*) Comparer NETTO, *Substitutionentheorie*, p. 87.

deux substitutions quelconques de la forme $U_\alpha\Sigma_\beta\Sigma'_\gamma$ et $U_{\alpha'}\Sigma_{\beta'}\Sigma'_{\gamma'}$, égales ou inégales, fait partie du même ensemble que les premières. Or ce produit

$$(U_\alpha\Sigma_\beta\Sigma'_\gamma)(U_{\alpha'}\Sigma_{\beta'}\Sigma'_{\gamma'}) = U_\alpha\Sigma_\beta\Sigma'_\gamma U_{\alpha'}\Sigma_{\beta'}\Sigma'_{\gamma'}$$

peut s'écrire successivement, en utilisant les relations précédentes et posant

$$\Sigma'_\gamma U_{\alpha'} = U_\delta\Sigma'_\gamma, \qquad \Sigma'_\gamma\Sigma_{\beta'} = U_\varepsilon\Sigma_{\beta'}\Sigma'_\gamma, \qquad \Sigma_\beta U_\delta U_\varepsilon = U_\rho\Sigma_\beta,$$

sous la forme suivante :

$$U_\alpha\Sigma_\beta U_\delta\Sigma'_\gamma\Sigma_{\beta'}\Sigma'_{\gamma'} = U_\alpha\Sigma_\beta U_\delta U_\varepsilon\Sigma_{\beta'}\Sigma'_\gamma\Sigma'_{\gamma'} = (U_\alpha U_\rho)(\Sigma_\beta\Sigma_{\beta'})(\Sigma'_\gamma\Sigma'_{\gamma'})$$

ou bien encore $U_{\alpha''}\Sigma_{\beta''}\Sigma'_{\gamma''}$; il fait bien partie de l'ensemble considéré.

Je vais montrer maintenant que les substitutions de cet ensemble sont distinctes, c'est-à-dire qu'on ne peut avoir

$$U_\alpha\Sigma_\beta\Sigma'_\gamma = U_{\alpha'}\Sigma_{\beta'}\Sigma'_{\gamma'} \quad \text{que si} \quad \alpha = \alpha', \quad \beta = \beta', \quad \gamma = \gamma'.$$

Supposons que l'on ait en effet une telle égalité ; on en déduit

$$\Sigma'_\gamma\Sigma'^{-1}_{\gamma'} = \Sigma_\beta^{-1}U_\alpha^{-1}U_{\alpha'}\Sigma_{\beta'} ;$$

le premier membre représente une substitution du groupe H, le second du groupe G ; elles ne peuvent être égales que si elles appartiennent au groupe K, c'est-à-dire sont de la forme U_δ ; l'égalité

$$\Sigma'_\gamma\Sigma'^{-1}_{\gamma'} = U_\delta,$$

qui entraîne la suivante :

$$\Sigma'_\gamma = U_\delta\Sigma'_{\gamma'},$$

ne peut avoir lieu, d'après les hypothèses faites sur les substitutions Σ', que si $\gamma = \gamma'$ et $U_\delta = 1$; il en résulte :

$$\Sigma_\beta^{-1}U_\alpha^{-1}U_{\alpha'}\Sigma_{\beta'} = 1, \qquad \Sigma_\beta = U_\alpha^{-1}U_{\alpha'}\Sigma_{\beta'}$$

et, pour la même raison, cette dernière égalité exige que $\beta = \beta'$ et $\alpha = \alpha'$.

Nous voyons ainsi que les substitutions $U_\alpha\Sigma_\beta\Sigma'_\gamma$ sont toutes distinctes ; leur nombre est $\rho p p' = \frac{rr'}{\rho}$; c'est l'ordre du groupe constitué par ces substitutions.

Il admet les groupes G et H comme sous-groupes ; je dis que chacun d'eux, G par exemple, est un sous-groupe invariant, ou qu'il est permutable à toute substitution du groupe $(U_\alpha\Sigma_\beta\Sigma'_\gamma)$; en effet, la transformée de la substitution $S = U_{\alpha'}\Sigma_{\beta'}$ du groupe G par

$U_\alpha \Sigma_\beta \Sigma'_\gamma$ est

$$(U_\alpha \Sigma_\beta \Sigma'_\gamma)^{-1}(U_{\alpha'}\Sigma_{\beta'})(U_\alpha \Sigma_\beta \Sigma'_\gamma) = \Sigma'^{-1}_\gamma \Sigma_\beta^{-1} U_\alpha^{-1} U_{\alpha'} \Sigma_{\beta'} U_\alpha \Sigma_\beta \Sigma'_\gamma$$

et peut être ramenée, par des transformations analogues à celles que nous avons opérées précédemment, à la forme $U_\delta \Sigma_{\beta'}$, qui appartient au groupe G.

Enfin le groupe K, qui est un sous-groupe de G et de H, est sous-groupe invariant de chacun d'eux, de G par exemple, car la transformée de $U_{\alpha'}$ par $U_\alpha \Sigma_\beta$ est

$$(U_\alpha \Sigma_\beta)^{-1} U_{\alpha'} (U_\alpha \Sigma_\beta) = \Sigma_\beta^{-1} U_\alpha^{-1} U_{\alpha'} U_\alpha \Sigma_\beta$$

et se ramène à une substitution U_δ du groupe K.

Le théorème se trouve ainsi démontré.

10. Lorsqu'un groupe G contient un sous-groupe invariant G_1, on dit qu'il est *composé* ; on dit qu'il est *simple* dans le cas contraire.

S'il n'existe aucun groupe H, sous-groupe invariant de G, et contenant G_1 comme sous-groupe, on dit que G_1 est un sous-groupe invariant maximum de G.

Si un groupe G est composé, et si l'on forme une suite de groupes

$$G, G_1, G_2, \ldots, G_\mu, 1,$$

dont chacun est un sous-groupe invariant maximum du précédent, et dont le dernier est formé de la substitution unité, on dit qu'elle est une suite de composition du groupe G.

$$\text{Si } r, \quad r_1 = \frac{r}{e_1}, \quad r_2 = \frac{r_1}{e_2}, \quad \ldots, \quad r_\mu = \frac{r_{\mu-1}}{e_\mu}, \quad r_{\mu+1} = \frac{r_\mu}{e_{\mu+1}} = 1$$

sont les ordres respectifs de ces groupes, les nombres $e_1, e_2, \ldots, e_\mu, e_{\mu+1}$ sont appelés les facteurs de composition de G ; on a $r = e_1 e_2 \ldots e_\mu e_{\mu+1}$.

Il peut se faire qu'un groupe composé ait plusieurs suites de composition distinctes ; nous allons démontrer le théorème fondamental suivant :

Théorème. — *S'il existe plusieurs suites de composition distinctes d'un groupe composé, les facteurs de composition sont les mêmes, à l'ordre près, et par suite sont en même nombre.*

Soient

(1) $$G \quad G_1 \quad G_2 \quad \ldots \quad G_\mu \quad 1,$$

(2) $$G \quad G'_1 \quad G'_2 \quad \ldots \quad G'_{\mu'} \quad 1$$

deux suites de composition de G ; $e_1, e_2, \ldots$; $e'_1, e'_2, \ldots$ les facteurs de composition. Il peut se faire que plusieurs groupes à partir de G soient les mêmes dans les deux suites ; il suffit de démontrer la proposition pour le premier groupe dont les sous-groupes sont différents ; je suppose, pour fixer les idées, que ce soit G, et que G_1 et G'_1 soient distincts. Considérons ces deux groupes :

$$G_1 = (S_1 = 1, \quad S_2, \quad \ldots, \quad S_{r_1}),$$

$$G'_1 = (T_1 = 1, \quad T_2, \quad \ldots, \quad T'_{r'_1})$$

et le groupe

$$K = (U_1 = 1, \quad U_2, \quad \ldots, \quad U_\rho)$$

formé par les substitutions communes. En employant les notations du § précédent, G_1 et G'_1 sont permutables et le groupe $(U_\alpha \Sigma_\beta \Sigma'_\gamma)$ les contient comme sous-groupes invariants ; je dis qu'il se confond avec le groupe G ; en effet, il est permutable au groupe G, car si V est une substitution de G, on a

$$V^{-1}(U_\alpha \Sigma_\beta \Sigma'_\gamma)V = V^{-1}U_\alpha \Sigma_\beta \Sigma'_\gamma V = (V^{-1}U_\alpha \Sigma_\beta V)(V^{-1}\Sigma'_\gamma V).$$

Comme la première parenthèse $V^{-1}U_\alpha \Sigma_\beta V$ est la transformée d'une substitution S, elle appartient au groupe G_1 et a la forme $U_{\alpha'}\Sigma_{\beta'}$; de même la seconde $V^{-1}\Sigma'_\gamma V$ appartient au groupe G'_1 et a la forme $U_{\alpha''}\Sigma'_{\gamma'}$; leur produit se ramène, comme on l'a vu, à $U_\delta \Sigma_{\beta'} \Sigma'_{\gamma'}$ où δ est convenablement choisi, et fait partie du même groupe $(U_\alpha \Sigma_\beta \Sigma'_\gamma)$; si donc ce groupe ne se confondait pas avec G, ce serait un sous-groupe invariant de G admettant G_1 et G'_1 comme sous-groupes, ce qui est impossible car G_1 et G'_1 sont maxima.

On déduit de là que $\rho p p' = r = r_1 e_1 = r'_1 e'_1$, et par suite que $p' = e_1, \quad p = e'_1, \quad \rho = \dfrac{r}{e_1 e'_1} = \dfrac{r_1}{e'_1} = \dfrac{r'_1}{e_1}.$

D'autre part, le groupe K dont nous venons de déterminer l'ordre est un sous-groupe invariant de G_1 ; je dis qu'il est maximum. S'il existait en effet un sous-groupe invariant de G_1 contenant K, soit H, il serait de la forme $H = (U_\alpha \sigma_\beta)$, où les subtitutions σ formeraient une partie de l'ensemble des substitutions Σ ; le théorème sur lequel nous nous sommes appuyé étant applicable aux groupes H et G'_1, qui sont permutables l'un à l'autre puisque chacun d'eux est une partie de G, on pourrait former un groupe $(U_\alpha \sigma_\beta \Sigma'_\gamma)$ permutable à G et contenant G'_1 comme sous-groupe, ce qui est impossible

puisque G'_1 est maximum ; le groupe H n'existe donc pas, et K est un sous-groupe invariant maximum de G_1 et aussi de G'_1.

De là résulte que si

$$K\ K_1\ K_2 \ldots 1$$

est une suite de composition de K, les deux suites

$$(3) \qquad G\ G_1\ K\ K_1 \ldots 1,$$

$$(4) \qquad G\ G'_1\ K\ K'_1 \ldots 1$$

sont deux suites de composition du groupe G.

Le théorème énoncé se déduit de là immédiatement ; il est vrai pour les suites (3) et (4), car les deux premiers facteurs de composition sont respectivement e_1, e'_1 ; e'_1, e_1, et les suivants sont identiques ; il sera vrai pour les suites primitives (1) et (2) s'il l'est pour (1) et (3) d'une part, (2) et (4) de l'autre ; or ces suites ont respectivement un groupe commun de plus que les premières à partir du groupe G, et l'on peut répéter le raisonnement de proche en proche jusqu'à ce qu'on obtienne des suites identiques ; le théorème est ainsi démontré.

11. Théorème. — *Le groupe alterné de n éléments est simple pour $n > 4$.*

Supposons que le groupe alterné soit composé et contienne un sous-groupe invariant

$$H = (S_1 S_2 \ldots) ;$$

je dis que ce sous-groupe contient au moins une substitution circulaire d'ordre 3 ; je vais montrer, pour le faire voir, qu'on peut toujours former une telle substitution appartenant au groupe.

Si l'on en connaît une, la proposition est évidente ; si l'on connaît une substitution renfermant plus de trois éléments dans un de ses cycles, par exemple

$$S = (x_1 x_2 x_3 x_4 \quad \ldots)(x_h \quad \ldots) \quad \ldots,$$

on la transformera par la substitution $\Sigma = (x_1 x_2 x_3)$ du groupe alterné, la transformée appartiendra au groupe H par hypothèse, et le produit

$$S^{-1}(\Sigma^{-1} S \Sigma) = (x_1 x_2 x_4)$$

répondra à la question ; si l'on connaît une substitution renfermant au moins un cycle de trois éléments, par exemple

$$S = (x_1 x_2 x_3)(x_4 x_5 x_6) \quad \ldots \qquad \text{ou} \qquad S = (x_1 x_2 x_3)(x_4 x_5) \quad \ldots,$$

on la transformera par $\Sigma_1 = (x_1x_2x_4)$, et le produit

$$T = S^{-1}(\Sigma_1^{-1}S\Sigma_1) = (x_1x_2x_5x_3x_4)$$

rentrera dans le cas précédent, de sorte que, en posant $\Sigma_2 = (x_1x_2x_5)$, on aura

$$T^{-1}\Sigma_2^{-1}T\Sigma_2 = (x_1x_2x_3),$$

qui sera une substitution circulaire d'ordre 3 ; si maintenant on connaît une substitution contenant au moins trois transpositions, telle que

$$S = (x_1x_2)(x_3x_4)(x_5x_6) \qquad \ldots,$$

en la transformant par $\Sigma_3 = (x_1x_3x_5)$, on aura

$$S^{-1}\Sigma_3^{-1}S\Sigma_3 = (x_1x_3x_5)(x_2x_6x_4),$$

ce qui rentrera dans un cas précédent ; enfin si l'on connaît une substitution

$$S = (x_1x_2)(x_3x_4)$$

qui soit le produit de deux transpositions, en la transformant par Σ_3 on aura

$$S^{-1}\Sigma_3^{-1}S\Sigma_3 = (x_1x_3x_5x_4x_2),$$

ce qui donnera une substitution déjà examinée.

Il y a donc toujours dans le sous-groupe invariant H au moins une substitution circulaire d'ordre trois ; si c'est par exemple

$$S = (x_1x_2x_3),$$

on a en transformant S^2 par $\Sigma_\alpha = (x_3x_2x_\alpha)$,

$$\Sigma_\alpha^{-1}S^2\Sigma_\alpha = (x_1x_2x_\alpha) ;$$

le groupe H contient par suite toutes les substitutions circulaires de la forme précédente, et d'après une propriété démontrée (§ 5) se confond avec le groupe alterné lui-même ; celui-ci est donc simple, comme nous l'avions annoncé, puisqu'il ne contient aucun sous-groupe invariant distinct de lui-même.

Remarque. — On voit que le raisonnement ne s'applique pas, dans le cas de $n = 4$, lorsque le groupe ne renferme que des substitutions de la forme $(x_1x_2)(x_3x_4)$, car on a utilisé un cinquième élément x_5 pour former la substitution Σ_3. Il y a ici un cas d'exception, et le groupe alterné de quatre éléments est composé ; nous avons vu en effet (§ 8) que ce groupe a un sous-groupe invariant

$$H = [1, \quad (x_1x_2)(x_3x_4), \quad (x_1x_3)(x_2x_4), \quad (x_1x_4)(x_2x_3)],$$

de sorte que la suite de composition du groupe alterné se compose : 1° du groupe alterné G′ ; 2° du groupe H ; 3° du groupe $K_1 = [1, (x_1x_2)(x_3x_4)]$ ou de l'un des groupes analogues K_2, K_3 ; 4° de la substitution unité.

Corollaire. — *La suite de composition du groupe symétrique de n éléments, pour* $n > 4$, *se compose de ce groupe, du groupe alterné, et de la substitution unité.*

Nous avons vu en effet au § 8 que le groupe alterné est un sous-groupe invariant du groupe symétrique ; il n'en existe pas d'autre, car un raisonnement identique au précédent montre que, pour $n > 4$, tout sous-groupe invariant du groupe symétrique doit renfermer toutes les substitutions circulaires d'ordre 3, et contenir par suite le groupe alterné ; comme il n'existe aucun groupe d'ordre inférieur à $n\,!$ et supérieur à $\frac{n\,!}{2}$, le seul sous-groupe invariant du groupe symétrique est le groupe alterné lui-même ; comme ce dernier est simple, la proposition est démontrée.

Les facteurs de composition sont, dans ce cas, 2 et $\frac{n\,!}{2}$.

Dans le cas de $n = 4$, la suite de composition du groupe symétrique est formée : 1° du groupe symétrique G ; 2° du groupe alterné G′ ; 3° du groupe H d'ordre 4 ; 4° de l'un des groupes K_1, K_2, K_3 d'ordre 2 ; 5° de la substitution unité.

Les facteurs de composition sont 2, 3, 2 et 2 ; le groupe H est de plus un sous-groupe invariant du groupe symétrique.

CHAPITRE III

DES FONCTIONS RATIONNELLES DE PLUSIEURS VARIABLES INDÉPENDANTES

12. Soit $\varphi(x_1, x_2, \ldots, x_n)$ une fonction entière des n variables indépendantes $x_1, x_2, \ldots, x_n$; effectuons sur ces variables toutes les substitutions possibles ; si les valeurs que prend la fonction sont algébriquement identiques à la première, on dit qu'elle est une fonction symétrique des n variables. On sait que toute fonction symétrique entière peut se mettre d'une seule manière sous la forme d'une fonction entière des fonctions symétriques simples :

$$f_1 = \Sigma x_i, \qquad f_2 = \Sigma x_i x_j, \qquad \ldots, \qquad f_n = x_1 x_2 \ldots x_n.$$

Il arrive le plus souvent que les valeurs algébriques prises par la fonction donnée ne sont pas toutes identiques ; soient

$$\varphi_1(x_1, \quad x_2, \quad \ldots, \quad x_n), \qquad \varphi_2, \qquad \ldots, \qquad \varphi_\rho$$

les fonctions distinctes obtenues, φ_1 représentant la fonction donnée ; il existe au moins une substitution conservant à φ_1 sa valeur, c'est la substitution unité ; dans tous les cas, les substitutions la laissant invariable forment un groupe, car en effectuant successivement un nombre quelconque de ces substitutions, la fonction conservera la même valeur, par conséquent le produit d'un nombre quelconque de substitutions de l'ensemble fait partie de cet ensemble ; le groupe dont nous venons de démontrer l'existence s'appelle le groupe de la fonction $\varphi_1(x_1, x_2, \ldots, x_n)$.

Par exemple, pour $n = 4$, la fonction $\varphi_1 = x_1x_2 + x_3x_4$ prend, pour toutes les substitutions, les trois valeurs φ_1, $\varphi_2 = x_1x_3 + x_2x_4$,

$\varphi_3 = x_1x_4 + x_2x_3$; φ_1 reste invariable pour les substitutions du groupe d'ordre 8 :

$$G_1 = [1, \ (x_1x_2), \ (x_3x_4), \ (x_1x_2)(x_3x_4), \ (x_1x_3)(x_2x_4), \ (x_1x_4)(x_2x_3), \ (x_1x_3x_2x_4), \ (x_1x_4x_2x_3)].$$

13. Réciproquement, on peut former, d'une infinité de manières, une fonction entière qui reste invariable pour les substitutions d'un groupe donné, et change de valeur pour toute autre substitution.

Pour le montrer, nous allons d'abord former une fonction entière des n variables prenant $n!$ valeurs distinctes pour les $n!$ substitutions ; la somme

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n,$$

où $u_1, u_2, \ldots, u_n$ sont des constantes arbitraires distinctes, répond à la question. Si l'on effectue en effet deux substitutions quelconques différentes :

$$S = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{a_1} & x_{a_2} & \ldots & x_{a_n} \end{pmatrix}, \qquad T = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{b_1} & x_{b_2} & \ldots & x_{b_n} \end{pmatrix},$$

dont nous représentons les inverses par

$$S^{-1} = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{\alpha_1} & x_{\alpha_2} & \ldots & x_{\alpha_n} \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{\beta_1} & x_{\beta_2} & \ldots & x_{\beta_n} \end{pmatrix},$$

les valeurs que prend la somme ψ_1 :

$$\psi_S = (u_1x_{a_1} + u_2x_{a_2} + \cdots + u_nx_{a_n}),$$
$$\psi_T = (u_1x_{b_1} + u_2x_{b_2} + \cdots + u_nx_{b_n}),$$

peuvent s'écrire, en les ordonnant par rapport à $x_1, x_2, \ldots, x_n$:

$$\psi_S = (u_{\alpha_1}x_1 + u_{\alpha_2}x_2 + \cdots + u_{\alpha_n}x_n),$$
$$\psi_T = (u_{\beta_1}x_1 + u_{\beta_2}x_2 + \cdots + u_{\beta_n}x_n) ;$$

elles ne peuvent être identiques algébriquement que si l'on a à la fois

$$u_{\alpha_1} = u_{\beta_1}, \qquad u_{\alpha_2} = u_{\beta_2}, \qquad \ldots,$$

ce qui est impossible, puisque les constantes u sont distinctes et que les indices $\alpha_1, \alpha_2, \ldots, \alpha_n$ ne sont pas tous identiques aux indices correspondants $\beta_1, \beta_2, \ldots, \beta_n$. ψ_S et ψ_T sont donc distinctes.

Nous appellerons la fonction précédente ψ_1 la fonction de Galois relative aux n variables $x_1, x_2, \ldots, x_n$.

Si maintenant on considère un groupe

$$G = (S_1 = 1, \quad S_2, \quad \ldots, \quad S_r)$$

et les valeurs $\psi_1, \psi_2, \ldots, \psi_r$ de la fonction de Galois lorsqu'on effectue les r substitutions du groupe, le produit

$$\varphi(u, \quad x_1, \quad \ldots, \quad x_n) = (u - \psi_1)(u - \psi_2)\ldots(u - \psi_r)$$

satisfait, quel que soit $u \neq 0$, à la condition d'avoir pour groupe le groupe donné G. En effet, si l'on effectue une substitution S_α du groupe, et si l'on pose

$$S_1S_\alpha = S_\alpha, \qquad S_2S_\alpha = S_\beta, \qquad \ldots, \qquad S_rS_\alpha = S_\lambda,$$

les substitutions $S_\alpha, S_\beta, \ldots, S_\lambda$ sont distinctes puisque $S_1, S_2, \ldots, S_r$ le sont, appartiennent au groupe G et par suite sont identiques, à l'ordre près, à $S_1, S_2, \ldots, S_r$; les fonctions $\psi_1, \psi_2, \ldots, \psi_r$ se changent, par la substitution S_α, en $\psi_\alpha, \psi_\beta, \ldots, \psi_\lambda$, qui sont identiques, à l'ordre près, aux premières valeurs ; par suite la fonction φ ne change pas.

D'autre part, si l'on effectue une substitution T n'appartenant pas au groupe et si l'on pose

$$S_1T = S_\mu, \qquad S_2T = S_\nu, \qquad \ldots, \qquad S_rT = S_\pi,$$

aucune des substitutions $S_\mu, S_\nu, \ldots, S_\pi$ ne fait partie du groupe G ; le produit φ se transforme en un nouveau produit

$$\varphi_T = (u - \psi_\mu)(u - \psi_\nu)\ldots(u - \psi_\pi),$$

qui est différent du premier ; en effet, si les produits φ et φ_T décomposés en facteurs linéaires par rapport aux variables x étaient égaux, chaque facteur de l'un serait égal, à une constante multiplicative près, à un certain facteur de l'autre, et l'on aurait par exemple

$$u - \psi_\mu = k(u - \psi_\alpha) ;$$

mais alors on en déduirait, puisque la constante u a été supposée $\neq 0$, $k = 1$ et $\psi_\alpha = \psi_\mu$, ce qui est impossible ; la proposition se trouve ainsi démontrée (*).

(*) Le raisonnement ne s'applique plus lorsque $u = 0$, à moins de supposer que les coefficients $u_1, u_2, \ldots, u_n$ de la fonction de Galois satisfont à d'autres conditions qu'à celle d'être inégaux. Considérons par exemple, dans le cas de $n = 4$, la fonction de Galois $\psi_1 = x_1 + ix_2 - x_3 - ix_4$, et le groupe H du § 8 ; le produit

$$\varphi = \psi_1\psi_2\psi_3\psi_4 = (x_1 + ix_2 - x_3 - ix_4)(x_2 + ix_1 - x_4 - ix_3)(x_3 + ix_4 - x_1 - ix_2)(x_4 + ix_3 - x_2 - ix_1)$$

Nous verrons plus loin quelles relations existent entre les fonctions, dont nous venons de démontrer l'existence, restant invariables pour les substitutions d'un groupe donné, et pour celles-là seulement ; nous dirons que ces fonctions appartiennent au groupe.

14. Soit $\varphi_1(x_1, x_2, \ldots, x_n)$ une fonction entière non symétrique appartenant à un groupe G_1 d'ordre r,

$$G_1 = (S_1 = 1, \quad S_2, \quad \ldots, \quad S_r),$$

$\varphi_2, \ldots, \varphi_\rho$ toutes les autres valeurs que prend φ_1, obtenues en lui appliquant par exemple les substitutions $\Sigma_2, \ldots, \Sigma_\rho$ non contenues dans le groupe précédent.

Considérons les substitutions de l'ensemble

$$S_1\Sigma_2, \qquad S_2\Sigma_2, \qquad \ldots, \qquad S_r\Sigma_2\,;$$

elles transforment toutes φ_1 en φ_2, et ce sont les seules, car si T est une substitution opérant cette transformation, le produit $T\Sigma_2^{-1}$ ne change pas φ_1 et est égal à l'une des substitutions S_k, de sorte que $T = S_k\Sigma_2$. On voit de même que les substitutions

$$S_1\Sigma_3, \qquad S_2\Sigma_3, \qquad \ldots, \qquad S_r\Sigma_3$$

changent φ_1 en φ_3 et sont les seules, et ainsi de suite.

Le tableau suivant, où Σ_1 représente la substitution unité,

$$\left\{\begin{array}{llll} S_1\Sigma_1, & S_2\Sigma_1, & \ldots, & S_r\Sigma_1, \\ S_1\Sigma_2, & S_2\Sigma_2, & \ldots, & S_r\Sigma_2, \\ \ldots & \ldots & \ldots & \ldots \\ S_1\Sigma_\rho, & S_2\Sigma_\rho, & \ldots, & S_r\Sigma_\rho, \end{array}\right.$$

renferme toutes les substitutions possibles, puisque la fonction prend, pour une substitution quelconque, l'une des ρ valeurs dont elle est susceptible, et que l'on a formé toutes celles qui lui font acquérir ces ρ valeurs ; elles sont toutes distinctes, car celles d'une

---

est bien invariable par les substitutions de H ; si on lui applique la substitution circulaire $T = (x_1x_2x_3x_4)$, on obtient la valeur

$\varphi_T = \psi_1'\psi_2'\psi_3'\psi_4' = (x_2+ix_3-x_4-ix_1)(x_3+ix_2-x_1-ix_4)(x_4+ix_1-x_2-ix_3)(x_1+ix_4-x_3-ix_2)$,

qui est identique à la première, car

$$\psi_1' = -i\psi_1, \qquad \psi_2' = i\psi_2, \qquad \psi_3' = -i\psi_3, \qquad \psi_4' = i\psi_4\,;$$

la fonction φ appartient donc à un groupe plus général que le groupe H.

La règle donnée par différents auteurs, par M. Serret et M. Jordan par exemple, n'est pas énoncée d'une manière assez précise.

même ligne le sont déjà, et si l'on avait d'autre part $S_h\Sigma_k = S_{h'}\Sigma_{k'}$ pour $k \neq k'$, on en déduirait $\Sigma_{k'} = S_{h'}^{-1}S_h\Sigma_k$; $\Sigma_{k'}$ transformerait φ_1 en φ_k et non en $\varphi_{k'}$ contrairement à l'hypothèse.

Par suite le tableau renferme une seule fois chacune des $n\,!$ substitutions, et l'on a $r\rho = n\,!$. On peut remarquer qu'il est analogue au tableau (4) du § 6, et l'on peut énoncer le théorème suivant :

Théorème. — *Si une fonction appartient à un groupe d'ordre* r, *elle a* $\rho = \dfrac{n\,!}{r}$ *valeurs, et il existe* r *substitutions qui la transforment dans chacune de ces* ρ *valeurs.*

Remarque. — La fonction φ_1 appartient au groupe G_1 d'ordre r; chacune des autres valeurs, par exemple φ_k, est une fonction qui prend ρ valeurs comme φ_1, et précisément ce sont $\varphi_1, \varphi_2, \ldots, \varphi_\rho$; en effet, une substitution quelconque S peut s'écrire $S = \Sigma_k^{-1}S'$; Σ_k^{-1} change φ_k en φ_1 et S' change φ_1 en une des ρ valeurs précédentes.

φ_k a alors un groupe G_k d'ordre r puisque c'est une fonction ayant ρ valeurs, et que $n\,! = r\rho$; je dis que ce groupe est le transformé de G_1 par Σ_k, c'est-à-dire que

$$G_k = \Sigma_k^{-1}G_1\Sigma_k\,;$$

en effet, considérons une substitution quelconque $\Sigma_k^{-1}S_\alpha\Sigma_k$ du groupe transformé de G_1 et appliquons-la à la fonction φ_k; Σ_k^{-1} la remplace par φ_1 que conserve S_α, et Σ_k transforme φ_1 en φ_k ; toutes les substitutions de ce groupe transformé laissent donc φ_k invariable, et font partie du groupe G_k de cette fonction ; comme leur nombre r est égal à l'ordre de ce dernier groupe, G_k est identique au groupe transformé lui-même, d'où ce résultat :

Corollaire. — *Les* ρ *valeurs d'une fonction ont chacune un groupe d'ordre* $r = \dfrac{n\,!}{\rho}$; *les groupes correspondant à deux d'entre elles sont transformés l'un de l'autre par la substitution qui remplace ces valeurs l'une par l'autre.*

15. Théorème. — *Toute fonction symétrique entière des valeurs distinctes que prend une fonction entière de plusieurs variables pour toutes les substitutions est une fonction symétrique entière de ces variables.*

Soient $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ les valeurs distinctes que prend une fonction entière φ_1 et $F(\varphi_1, \varphi_2, \ldots, \varphi_\rho)$ une fonction symétrique entière de ces ρ valeurs; c'est une fonction entière des variables restant invariable pour toute substitution. En effet, une substitution quelconque S a pour résultat de conserver à chaque fonction sa valeur ou de la remplacer par une des autres ; les nouvelles valeurs $\varphi'_1, \varphi'_2, \ldots, \varphi'_\rho$ qu'elles prennent sont toutes distinctes, car si l'on avait $\varphi'_h = \varphi'_k$, en effectuant la même substitution S^{-1} sur les deux membres, les résultats φ_h et φ_k devraient être égaux, ce qui est impossible ; par conséquent les fonctions φ se reproduisent après la substitution S, dans un ordre quelconque, et la fonction symétrique entière $F(\varphi_1, \varphi_2, \ldots, \varphi_\rho)$ conserve la même valeur ; c'est donc une fonction symétrique des variables x.

Corollaire. — *Les ρ valeurs que prend une fonction entière de plusieurs variables pour toutes les substitutions sont racines d'une équation algébrique entière dont les coefficients sont des polynomes entiers par rapport aux fonctions symétriques simples de ces variables.*

En effet, les coefficients de l'équation

$$\varphi(z) = (z-\varphi_1)(z-\varphi_2)\ldots(z-\varphi_\rho) = z^\rho + A_1 z^{\rho-1} + \cdots + A_\rho = 0$$

ayant pour racines les ρ valeurs $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ sont des fonctions symétriques entières de ces ρ valeurs et par suite s'expriment par des polynomes entiers par rapport aux fonctions symétriques simples $f_1, f_2, \ldots, f_n$ des n variables x ; on peut ajouter que le premier coefficient de l'équation est égal à l'unité.

Comme exemple de ce qui précède, considérons, dans le cas de $n = 4$, la fonction $\varphi_1 = x_1x_2 + x_3x_4$; elle admet le groupe d'ordre 8

$$G_1 = [1,\ (x_1x_2),\ (x_3x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3),\ (x_1x_3x_2x_4),\ (x_1x_4x_2x_3)]$$

et a par suite trois valeurs ; les deux autres sont

$$\varphi_2 = x_1x_3 + x_2x_4,$$

déduite de la première par $\Sigma_2 = (x_2x_3)$, et appartenant au groupe

$$G_2 = \Sigma_2^{-1}G_1\Sigma_2 = [1,\ (x_1x_3),\ (x_2x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_4)(x_2x_3),\ (x_1x_2x_3x_4),\ (x_1x_4x_3x_2)],$$

et

$$\varphi_3 = x_1x_4 + x_2x_3,$$

déduite de φ_1 par $\Sigma_3 = (x_2 x_4)$, et appartenant au groupe

$$G_3 = \Sigma_3^{-1} G_1 \Sigma_3 = [1, \ (x_1x_4), \ (x_2x_3), \ (x_1x_4)(x_2x_3), \ (x_1x_3)(x_2x_4), \ (x_1x_2)(x_3x_4), \ (x_1x_3x_4x_2), \ (x_1x_2x_4x_3)].$$

On peut remarquer que les trois groupes ont en commun le sous-groupe

$$H = [1, \ (x_1x_2)(x_3x_4), \ (x_1x_3)(x_2x_4), \ (x_1x_4)(x_2x_3)];$$

mais c'est un fait exceptionnel sur lequel nous reviendrons.

Les trois fonctions φ_1, φ_2, φ_3 ont pour fonctions symétriques simples les valeurs suivantes, où l'on pose

$$f_1 = \Sigma x_i, \qquad f_2 = \Sigma x_i x_j, \qquad f_3 = \Sigma x_i x_j x_k, \qquad f_4 = x_1 x_2 x_3 x_4,$$

$$\varphi_1 + \varphi_2 + \varphi_3 = \Sigma x_i x_j = f_2,$$

$$\varphi_1\varphi_2 + \varphi_1\varphi_3 + \varphi_2\varphi_3 = \Sigma x_i^2 x_j x_k = (\Sigma x_i)(\Sigma x_i x_j x_k) - 4x_1x_2x_3x_4 = f_1 f_3 - 4f_4,$$

$$\varphi_1\varphi_2\varphi_3 = \Sigma x_i^2 x_j^2 x_k^2 + x_1x_2x_3x_4 \Sigma x_i^2 = f_3^2 - 4f_2f_4 + f_1^2 f_4,$$

de sorte qu'elles sont racines de l'équation du troisième degré

$$z^3 - f_2 z^2 + (f_1 f_3 - 4f_4)z - (f_3^2 - 4f_2f_4 + f_1^2 f_4) = 0.$$

On peut remarquer que le discriminant de cette équation est

$$(\varphi_1 - \varphi_2)^2(\varphi_1 - \varphi_3)^2(\varphi_2 - \varphi_3)^2 = (x_1 - x_4)^2(x_2 - x_3)^2 (x_1 - x_3)^2(x_2 - x_4)^2(x_1 - x_2)^2(x_3 - x_4)^2$$

et qu'il est identique au discriminant de l'équation du quatrième degré qui aurait pour racines x_1, x_2, x_3 et x_4 (*).

16. Nous nous sommes occupés jusqu'ici des fonctions entières de plusieurs variables ; nous pouvons rattacher à ce qui précède l'étude des fonctions rationnelles.

Soit $\dfrac{\varphi_1(x_1, x_2, \ldots, x_n)}{\psi_1(x_1, x_2, \ldots, x_n)}$ une fonction rationnelle mise sous la forme du quotient de deux fonctions entières des variables $x_1, x_2, \ldots, x_n$; on peut la remplacer par une autre dont le dénominateur soit une fonction symétrique entière de ces variables. Il suffit de considérer les valeurs algébriques distinctes que prend le dénominateur pour toutes les substitutions ; si $\psi_1, \psi_2, \ldots, \psi_\rho$ sont ces valeurs, leur pro-

---

(*) Cette remarque a été généralisée par Kronecker et M. Netto. Comparer Netto, *Substitutionentheorie*, p. 56.

duit est une fonction symétrique entière, et l'on peut remplacer la fraction par

$$\frac{\varphi_1\psi_2\psi_3\ldots\psi_\rho}{\psi_1\psi_2\psi_3\ldots\psi_\rho},$$

dont le dénominateur est symétrique et dont le numérateur est une fonction entière des variables ; si elle est elle-même symétrique, on dit que la fraction donnée est une fonction symétrique rationnelle, et on peut la mettre sous la forme du quotient de deux polynomes entiers par rapport aux fonctions symétriques simples ; si au contraire elle a ρ valeurs et appartient à un groupe G, on dit qu'il en est de même de la fraction donnée ; les ρ valeurs de la fraction sont racines d'une équation algébrique à coefficients entiers par rapport aux fonctions symétriques simples, le premier n'étant plus égal à l'unité ; plus généralement, tout ce que nous avons dit des fonctions entières s'applique aux fonctions rationnelles.

CHAPITRE IV

RELATIONS ALGÉBRIQUES ENTRE LES FONCTIONS RATIONNELLES DE PLUSIEURS VARIABLES

17. Nous avons vu au chapitre précédent que chaque fonction entière ou rationnelle de n variables indépendantes $x_1, x_2, \ldots, x_n$ appartient à un groupe particulier, et que, réciproquement, on peut former une infinité de fonctions entières ou rationnelles appartenant à un groupe donné. Ces fonctions ne sont pas indépendantes, comme cela résulte du théorème suivant, démontré par Lagrange pour la première fois.

Théorème. — *Si deux fonctions rationnelles de plusieurs variables sont telles que l'une reste invariable pour toutes les substitutions du groupe auquel l'autre appartient, la première s'exprime au moyen de la seconde sous forme d'un polynome entier dont les coefficients sont des fonctions symétriques des variables.*

Soit φ_1 une fonction entière ou rationnelle appartenant au groupe

$$G_1 = (S_1 = 1, \quad S_2, \ldots, S_r)$$

et ayant $\rho = \dfrac{n\,!}{r}$ valeurs, $\varphi_1, \varphi_2, \ldots, \varphi_\rho$, déduites de la première par les substitutions $\Sigma_1 = 1, \quad \Sigma_2, \ldots, \Sigma_\rho$; ces valeurs sont racines d'une équation algébrique de degré ρ :

$$\Phi(z) = (z - \varphi_1)(z - \varphi_2)\ldots(z - \varphi_\rho) = 0,$$

dont les coefficients sont des fonctions symétriques des variables.

Soit maintenant ψ_1 une autre fonction restant invariable pour toutes les substitutions de G_1 ; elle a un groupe identique à G_1 ou le contenant comme sous-groupe ; supposons, pour nous placer

dans le cas le plus général, que ψ_1 appartienne à un groupe H_1 d'ordre $r' = kr$, de sorte que pour toutes les substitutions, ψ_1 prenne $\rho' = \frac{n!}{r'} = \frac{\rho}{k}$ valeurs, $\psi_1, \psi_2, \ldots, \psi_{\rho'}$.

Reprenons le tableau des $n!$ substitutions dont nous avons parlé au § 14

$$\begin{array}{llll} S_1\Sigma_1, & S_2\Sigma_1, & \ldots, & S_r\Sigma_1 \\ S_1\Sigma_2, & S_2\Sigma_2, & \ldots, & S_r\Sigma_2 \\ \cdots & \cdots & \cdots & \cdots \\ S_1\Sigma_\rho, & S_2\Sigma_\rho, & \ldots, & S_r\Sigma_\rho \end{array}$$

tel que celles de la k^e ligne changent φ_1 en φ_k, et appliquons-les à ψ_1 ; comme toutes les substitutions d'une même ligne produisent sur ψ_1 le même effet, et qu'à chacune des ρ' valeurs de cette fonction doivent correspondre kr substitutions, il est nécessaire que le tableau précédent se décompose en ρ' ensembles de k lignes chacun, transformant respectivement ψ_1 en $\psi_1, \psi_2, \ldots, \psi_{\rho'}$. Nous désignerons cependant par $\psi_1, \psi_2, \ldots, \psi_\rho$ les valeurs que prend ψ_1 lorsqu'on lui applique les substitutions $\Sigma_1, \Sigma_2, \ldots, \Sigma_\rho$, ces valeurs n'étant pas toutes distinctes mais égales k à k.

On peut ajouter que si les k premières lignes du tableau par exemple ne changent pas ψ_1 et constituent le groupe H_1, les autres ensembles de k lignes relatifs aux valeurs distinctes de ψ_1 s'obtiendront en multipliant les substitutions de H_1 par des substitutions $T_2, T_3, \ldots, T_{\rho'}$, convenablement choisies.

Cela posé, soit $F_i(\varphi_i, \psi_i)$ une fonction rationnelle de φ_i et ψ_i, et considérons une fonction symétrique des valeurs $F_1, F_2, \ldots, F_\rho$; c'est une fonction symétrique des variables x, car si une substitution S change φ_i en φ_j, elle change également ψ_i en ψ_j, elle conserve donc à chaque fonction F sa valeur ou la transforme dans une des autres ; d'après un raisonnement déjà fait au § 15, les valeurs des fonctions $F_1, F_2, \ldots, F_\rho$ se changent après une substitution quelconque en d'autres identiques aux premières, à l'ordre près, et toute fonction symétrique de ces valeurs est une fonction symétrique des variables.

Considérons alors la somme

$$\sum_{i=1}^{i=\rho} \psi_i \cdot \frac{\Phi(z)}{z - \varphi_i} \cdot \frac{1}{\Phi'(\varphi_i)};$$

d'après ce qui précède, c'est une fonction symétrique des variables x, et elle se met sous forme d'un polynome entier en z de degré $\rho - 1$ dont les coefficients sont des fonctions symétriques rationnelles des variables,

$$\Psi(z) = A_1 z^{\rho-1} + A_2 z^{\rho-2} + \cdots + A_\rho ;$$

d'autre part, d'après la formule de Lagrange, ce polynome en z prend la valeur ψ_i lorsqu'on remplace la variable par φ_i ; on a donc pour toute valeur de l'indice i,

$$\psi_i = \Psi(\varphi_i) = A_1 \varphi_i^{\rho-1} + A_2 \varphi_i^{\rho-2} + \cdots + A_\rho .$$

Nous avons ainsi démontré non seulement que ψ_1 s'exprime au moyen de φ_1 sous la forme d'un polynome entier de degré $\rho - 1$ à coefficients symétriques, mais encore qu'une valeur quelconque de ψ_1 s'exprime au moyen de la valeur correspondante de φ_1 par le même polynome.

Si nous supposons en particulier que les groupes de φ_1 et ψ_1 sont identiques, le raisonnement s'applique à chacune de ces fonctions, ce qui permet d'exprimer chacune d'elles en fonction entière de l'autre ; on énonce ordinairement ce résultat en disant que *deux fonctions de même groupe s'expriment rationnellement l'une par l'autre.*

Réciproquement, *si deux fonctions rationnelles s'expriment rationnellement l'une par l'autre, avec des coefficients symétriques, elles appartiennent au même groupe*, car chacune reste invariable pour les substitutions qui constituent le groupe de l'autre.

Les fonctions entières ou rationnelles de plusieurs variables se distinguent ainsi en genres, celles d'un même genre étant exprimables rationnellement au moyen de l'une quelconque d'entre elles ; c'est Kronecker qui a montré l'importance de cette notion de genre (Gattung) dans l'étude des fonctions algébriques ; il a appelé genres conjugués ceux auxquels appartiennent les différentes valeurs que prend une fonction rationnelle pour toutes les substitutions (*).

18. Comme application, considérons une fonction φ_1 ayant deux valeurs, φ_1 et φ_2, pour toutes les substitutions ; chacune d'elles a un groupe d'ordre $\frac{1}{2} n!$; en désignant ces deux groupes respective-

(*) KRONECKER, *Monatsberichte der Berliner Akademie*, 1879, p. 212.

ment par G_1 et G_2, je vais démontrer qu'ils sont identiques au groupe alterné.

En effet, soit S une substitution du groupe G_1 de φ_1, laissant cette fonction invariable; elle ne peut changer la valeur de φ_2, car sinon elle remplacerait φ_2 par φ_1 et son inverse S^{-1} remplacerait φ_1 par φ_2, ce qui est impossible puisque S^{-1} appartient comme S au groupe G_1; par conséquent toute substitution de G_1 fait partie de G_2, et ces deux groupes, qui ont le même ordre, sont identiques.

Le groupe G_1 commun à φ_1 et φ_2 est permutable au groupe symétrique; en effet, il l'est d'abord évidemment à toute substitution S de G_1; si maintenant Σ est une autre substitution n'appartenant pas à ce groupe, et remplaçant par suite φ_1 par φ_2 et φ_2 par φ_1, la transformée $\Sigma^{-1}S\Sigma$ de S par Σ ne change ni φ_1 ni φ_2 et fait partie du groupe G_1; ce dernier est dès lors un sous-groupe invariant du groupe symétrique et, d'après le raisonnement du § 11, c'est le groupe alterné.

La fonction

$$\psi = \sqrt{\Delta} = \Pi(x_i - x_j), \qquad i > j, \qquad i, j = 1, 2, \ldots, n$$

prend pour toutes les substitutions deux valeurs égales et de signes contraires, on dit qu'elle est alternée, et elle appartient au groupe précédent; elle est racine de l'équation $\psi^2 = \Delta$, où Δ est le discriminant; toute autre fonction à deux valeurs est alors de la forme $A + B\sqrt{\Delta}$, où A et B sont symétriques.

On peut démontrer ce qui précède d'une autre manière : si φ_1 et φ_2 sont les deux valeurs de la fonction, $\varphi_1 + \varphi_2$ est symétrique et $\varphi_1 - \varphi_2$ conserve sa valeur ou change de signe, car une substitution quelconque laisse φ_1 et φ_2 invariables ou les remplace l'une par l'autre; ce dernier cas se présente au moins pour une transposition $(x_\alpha x_\beta)$, par suite $\varphi_1 - \varphi_2$ s'annule pour $x_\alpha = x_\beta$ et est divisible par $x_\alpha - x_\beta$; en effectuant ensuite toutes les substitutions possibles, on voit que $\varphi_1 - \varphi_2$ est divisible par toutes les différences $x_i - x_j$, par conséquent par $\sqrt{\Delta}$.

Le quotient $\dfrac{\varphi_1 - \varphi_2}{\sqrt{\Delta}}$ est une fonction symétrique, par conséquent φ_1 et φ_2 sont de la forme $A + B\sqrt{\Delta}$ et $A - B\sqrt{\Delta}$, où A et B sont symétriques ; on conclut de là qu'elles appartiennent au même groupe que $\sqrt{\Delta}$, c'est-à-dire au groupe alterné.

19. Comme conséquence du théorème fondamental que nous venons de démontrer au § 17, nous pouvons énoncer les corollaires suivants :

Corollaire I. — *Étant données plusieurs fonctions entières ou rationnelles de plusieurs variables, on peut les exprimer au moyen d'une seule fonction nouvelle sous forme de polynomes entiers à coefficients symétriques.*

Soient $\varphi_1, \psi_1, \chi_1, \ldots$ plusieurs fonctions rationnelles, et

$$\omega_1 = u\varphi_1 + v\psi_1 + w\chi_1 + \cdots$$

une fonction linéaire et homogène des précédentes, avec des coefficients constants arbitraires ; nous supposons ces coefficients assujettis à la condition suivante, que l'on peut réaliser d'une infinité de manières : si l'on prend les valeurs $\varphi_1, \varphi_2, \ldots ; \psi_1, \psi_2, \ldots$ des fonctions données, une identité de la forme

$$u\varphi_h + v\psi_k + \cdots = u\varphi_{h'} + v\psi_{k'} + \cdots$$

n'est possible que si $h = h', \quad k = k', \quad \ldots$

Si cela a lieu, ω_1 reste invariable par les substitutions communes aux groupes de $\varphi_1, \psi_1, \ldots$ et change pour toute autre substitution ; elle appartient à un groupe contenu dans les précédents, par suite les fonctions $\varphi_1, \psi_1, \ldots$ s'expriment en fonction entière de ω_1 avec des coefficients symétriques.

On peut ajouter que les autres valeurs $\varphi_2, \varphi_3, \ldots, \psi_2, \ldots$ s'expriment de la même manière au moyen des autres valeurs de la fonction ω_1.

20. Un cas particulier est celui où les groupes des fonctions données n'ont aucune substitution commune ; le groupe de ω_1 se réduit à l'unité, et ω_1 change pour toute substitution.

Or la fonction de Galois déjà considérée au § 13,

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n,$$

remplit la condition d'avoir $n\,!$ valeurs, et son groupe, qui se réduit à l'unité, est contenu dans tout autre groupe, d'où ce résultat :

Corollaire II. — *Une fonction rationnelle quelconque de plusieurs variables s'exprime d'une manière entière au moyen d'une fonction*

particulière ayant n ! valeurs, en particulier au moyen de la fonction de Galois.

Corollaire III. — *Les n ! valeurs de la fonction de Galois sont des fonctions entières de l'une quelconque d'entre elles*, puisqu'elles appartiennent au même groupe ; on peut encore dire que *les genres conjugués fournis par les valeurs de la fonction de Galois sont confondus.*

Corollaire IV. — *Les variables elles-mêmes, $x_1, x_2, \ldots, x_n$, s'expriment d'une manière entière au moyen de la fonction de Galois.*

Le groupe auquel appartient x_1 par exemple est formé des $(n-1)$! substitutions renfermant les $n-1$ autres variables ; la fonction a ainsi n valeurs qui sont les variables elles-mêmes $x_1, x_2, \ldots, x_n$, et chacune d'elles s'exprime d'une manière entière au moyen de la fonction de Galois (*).

Le procédé indiqué par Galois pour exprimer les variables en fonction rationnelle d'une seule fonction est plus simple que le calcul fondé sur la formule de Lagrange ; ce dernier, que nous avons indiqué plus haut, a l'avantage cependant de donner une fonction entière et non rationnelle. Le calcul de Galois consiste, étant donnée une des variables, par exemple x_1, à prendre la fonction

$$\psi_1 = u_1x_1 + u_2x_2 + \ldots + u_nx_n$$

et les $(n-1)$! valeurs $\psi_1, \psi_2, \ldots, \psi_{[n-1]!}$ qu'elle prend pour les substitutions laissant x_1 fixe et changeant les autres éléments ; l'équation

$$\Phi_1(z) = (z-\psi_1)(z-\psi_2)\ldots(z-\psi_{(n-1)!}) = 0$$

qui les admet pour racines a ses coefficients fonctions symétriques de $x_2, x_3, \ldots, x_n$. On peut les exprimer en fonction entière de x_1 et des fonctions symétriques $f_1, f_2, \ldots, f_n$ des n variables, car si l'on pose

$$f(x) = (x-x_1)(x-x_2)\ldots(x-x_n),$$

ce sont des fonctions entières des coefficients de l'équation

$$\frac{f(x)}{x-x_1} = 0.$$

(*) On trouve dans Serret, *Algèbre supérieure*, t. II, p. 442, la démonstration qu'a donnée Galois de cette proposition, dans le t. XI du *Journal de Mathématiques*.

Soit donc $\Phi_1(z, x_1) = 0$ l'équation qui a pour racines les valeurs ψ_h considérées ; on a identiquement $\Phi_1(\psi_h, x_1) = 0$, de sorte que l'équation $\Phi_1(\psi_h, x) = 0$ a la racine $x = x_1$; je dis qu'elle n'est satisfaite par aucune autre des variables $x_2, x_3, \ldots, x_n$. Supposons en effet que l'on ait par exemple $\Phi_1(\psi_h, x_2) = 0$; l'équation $\Phi_1(z, x_2) = 0$ aurait pour racine ψ_h ; or le premier membre de cette dernière équation se déduit de $\Phi_1(z, x_1)$ en effectuant la transposition $T = (x_1 x_2)$, et s'annule pour les valeurs $\psi'_1, \psi'_2, \ldots$ obtenues en opérant cette transposition sur $\psi_1, \psi_2, \ldots$; on sait que les nouvelles valeurs ainsi formées sont toutes distinctes des premières, par conséquent on ne peut avoir $\Phi_1(\psi_h, x_2) = 0$.

On conclut de là que les équations $\Phi_1(\psi_h, x) = 0$ et $f(x) = 0$ ont une seule racine commune x_1 ; on l'obtiendra en cherchant le plus grand commun diviseur des premiers membres et continuant l'opération jusqu'à ce qu'on obtienne un reste du premier degré ; en l'annulant, on a la valeur de x_1 exprimée rationnellement au moyen de ψ_h et de $f_1, f_2, \ldots, f_n$; on peut remplacer naturellement ψ_h par une quelconque des $(n-1)!$ valeurs considérées.

Comme exemple, considérons trois variables, et la fonction de Galois

$$\psi_1 = x_1 + \omega x_2 + \omega^2 x_3,$$

où ω est une racine cubique imaginaire de l'unité ; pour exprimer x_1 nous prenons les deux valeurs ψ_1 et $\psi_2 = x_1 + \omega x_3 + \omega^2 x_2$; elles sont racines de l'équation

$$\Phi_1(z, x_1) = z^2 - (3x_1 - f_1)z + f_1^2 - 3f_2 = 0.$$

Le premier membre renferme x_1 au premier degré ; par suite il représente, lorsqu'on remplace z par ψ_1 ou ψ_2, le plus grand commun diviseur de $f(x_1)$ et de $\Phi_1(\psi_1, x_1)$ ou $\Phi_1(\psi_2, x_1)$, et l'on a immédiatement, en résolvant par rapport à x_1,

$$x_1 = \frac{\psi_1^2 + f_1\psi_1 + f_1^2 - 3f_2}{3\psi_1} = \frac{\psi_2^2 + f_1\psi_2 + f_1^2 - 3f_2}{3\psi_2}.$$

De même, en posant $\psi_3 = x_3 + \omega x_2 + \omega^2 x_1$, $\psi_4 = x_2 + \omega x_1 + \omega^2 x_3$, on a

$$x_2 = \frac{\omega\psi_1^2 + \omega^2 f_1\psi_1 + f_1^2 - 3f_2}{3\omega^2\psi_1} = \frac{\omega\psi_3^2 + \omega^2 f_1\psi_3 + f_1^2 - 3f_2}{3\omega^2\psi_3},$$

$$x_3 = \frac{\omega^2\psi_1^2 + \omega f_1\psi_1 + f_1^2 - 3f_2}{3\omega\psi_1} = \frac{\omega^2\psi_4^2 + \omega f_1\psi_4 + f_1^2 - 3f_2}{3\omega\psi_4}.$$

Un autre procédé de calcul indiqué par Kronecker à propos du problème général de l'élimination est le suivant (*) :

Soit ψ_1 la fonction de Galois déjà considérée, $\psi_1, \psi_2, \ldots, \psi_{n!}$ ses $n!$ valeurs pour toutes les substitutions; formons l'équation qui les admet pour racines :

$$F(z, u_1, u_2, \ldots, u_n, f_1, f_2, \ldots, f_n) = (z - \psi_1)(z - \psi_2) \ldots (z - \psi_{n!}) = 0.$$

Le premier membre est un polynome de degré $n!$ en z, dont les coefficients sont des fonctions entières des paramètres $u_1, u_2, \ldots, u_n$, et des fonctions symétriques simples $f_1, f_2, \ldots, f_n$; si l'on y remplace z par

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n,$$

il s'annule identiquement lorsqu'on le considère non seulement comme fonction de $x_1, x_2, \ldots, x_n$, mais encore comme fonction des paramètres laissés indéterminés $u_1, u_2, \ldots, u_n$, et sa dérivée par rapport à l'un d'eux est identiquement nulle. En prenant par exemple la dérivée par rapport à u_α, on a une équation,

$$x_\alpha \frac{\partial F}{\partial z} + \frac{\partial F}{\partial u_\alpha} = 0,$$

qui se transforme en identité lorsqu'on remplace z par ψ_1, et elle fournit précisément la valeur de x_α en fonction de ψ_1.

21. Nous avons exprimé dans ce qui précède une fonction rationnelle des variables, appartenant à un certain groupe, au moyen d'une autre fonction appartenant au même groupe ou à un autre contenu dans le premier ; nous allons résoudre la question inverse.

Théorème. — *Si une fonction appartient à un groupe* G *d'ordre* r *contenu dans un groupe* G' *d'ordre* $r' = mr$, *elle prend pour toutes les substitutions de* G' m *valeurs qui sont racines d'une équation d'ordre* m; *les coefficients de cette équation sont des fonctions entières à coefficients symétriques d'une fonction arbitrairement choisie appartenant à* G'.

Soit φ_1 une fonction appartenant au groupe

$$G = [S_1 = 1, \ S_2, \ldots, S_r];$$

(*) Comparer Borel et Drach, *Introduction à la théorie des Nombres et à l'Algèbre supérieure*, pages 205 et 241.

si on lui applique toutes les substitutions de G', et si elle prend des valeurs distinctes $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ par les substitutions $\Sigma = 1$, $\Sigma_2, \ldots, \Sigma_\rho$, on voit, comme au § 14, que les substitutions du tableau

$$(T) \quad \begin{cases} S_1\Sigma_1, & S_2\Sigma_1, & \ldots, & S_r\Sigma_1, \\ S_1\Sigma_2, & S_2\Sigma_2, & \ldots, & S_r\Sigma_2, \\ \ldots & \ldots & \ldots & \ldots \\ S_1\Sigma_\rho, & S_2\Sigma_\rho, & \ldots, & S_r\Sigma_\rho \end{cases}$$

sont distinctes et constituent le groupe G', de sorte que $\rho = m$; celles de la ligne de rang k changent φ_1 en φ_k, et ce sont les seules du groupe G' jouissant de cette propriété. Une substitution quelconque de ce tableau change $\varphi_1, \varphi_2, \ldots, \varphi_m$ en d'autres valeurs identiques aux premières, à l'ordre près, de sorte que les fonctions symétriques de ces m valeurs restent invariables par les substitutions de G' ; on pourra les exprimer, comme on l'a vu, sous forme entière au moyen d'une fonction ψ_1 arbitrairement choisie et appartenant au groupe G', les coefficients étant des fonctions symétriques des variables.

On peut ajouter que les groupes $G, \Sigma_2^{-1}G\Sigma_2, \ldots, \Sigma_m^{-1}G\Sigma_m$ contenus dans le groupe G' sont ceux auxquels appartiennent respectivement les valeurs $\varphi_1, \varphi_2, \ldots, \varphi_m$.

Les théorèmes du chapitre précédent ne sont que des cas particuliers de celui que nous venons de démontrer, et s'en déduisent en supposant que G' soit le groupe symétrique.

Pour donner un exemple, nous avons vu au § 12 que la fonction

$$\varphi_1 = x_1x_2 + x_3x_4$$

admet le groupe d'ordre 8 désigné par G_1 ; la fonction

$$\chi_1 = x_1 + x_2 - x_3 - x_4$$

admet le groupe d'ordre 4

$$g_1 = [1, \quad (x_1x_2), \quad (x_3x_4), \quad (x_1x_2)(x_3x_4)]$$

contenu dans le précédent ; c'est une fonction à six valeurs, qui prend, pour les substitutions de G_1, les deux valeurs χ_1 et $\chi_1' = -\chi_1$, dont les fonctions symétriques simples sont $\chi_1 + \chi_1' = 0$ et

$$\chi_1\chi_1' = -[x_1 + x_2 - x_3 - x_4]^2 = 4f_2 - f_1^2 - 4\varphi_1 ;$$

ces fonctions symétriques sont exprimées au moyen de φ_1, de sorte

que les deux valeurs χ_1, χ'_1 sont racines de l'équation

$$\chi^2+4f_2-f_1^2-4\varphi_1=0;$$

elles ont du reste le même groupe g_1.

Comme autre exemple, les trois groupes G_1, G_2, G_3 des trois fonctions φ_1, φ_2 et φ_3 du § 15 ont en commun le groupe

$$H=[1,(x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)]$$

auquel appartient la fonction à six valeurs

$$\omega_1=x_1x_2+x_3x_4-x_1x_3-x_2x_4=\varphi_1-\varphi_2,$$

les cinq autres étant

$$\omega_2=\varphi_1-\varphi_3,\quad \omega_3=\varphi_2-\varphi_3,\quad \omega_4=\varphi_2-\varphi_1,\quad \omega_5=\varphi_3-\varphi_1,\quad \omega_6=\varphi_3-\varphi_2.$$

Pour les substitutions du groupe G_1, ω_1 a les deux valeurs ω_1 et ω_2 dont les fonctions symétriques, exprimées au moyen de φ_1, sont

$$(1)\quad \begin{aligned}\omega_1+\omega_2&=2\varphi_1-(\varphi_2+\varphi_3)=3\varphi_1-f_2,\\ \omega_1\omega_2&=\varphi_1^2-\varphi_1(\varphi_2+\varphi_3)+\varphi_2\varphi_3=3\varphi_1^2-2\varphi_1f_2+f_1f_3-4f_4,\end{aligned}$$

de sorte que ω_1 et ω_2 sont les racines de l'équation

$$\omega^2-(3\varphi_1-f_2)\omega+(3\varphi_1^2-2\varphi_1f_2+f_1f_3-4f_4)=0;$$

on trouverait des équations analogues en partant de G_2 et G_3.

On remarque que les six valeurs de ω appartiennent au même groupe H; elles s'expriment par suite rationnellement l'une par l'autre; on aura par exemple la relation qui existe entre ω_1 et ω_2 en éliminant φ_1 entre les équations (1) et l'équation déjà formée au § 15,

$$\varphi_1^3-f_2\varphi_1^2+(f_1f_3-4f_4)\varphi_1-(f_3^2-4f_2f_4+f_1^2f_4)=0,$$

et écrivant que les deux équations ont en ω_2 une racine commune; on a ainsi

$$\omega_2=\frac{3\omega_1^3+A\omega_1+B}{6\omega_1^2+2A},$$

où

$$A=3f_1f_3-12f_4-f_2^2,$$

$$B=72f_2f_4-27f_1^2f_4-27f_3^2-2f_2^3+9f_1f_2f_3.$$

22. Dans les deux exemples précédents, les deux valeurs de χ_1 pour le groupe G_1 ont même groupe, et il en est de même des valeurs de ω_1; nous allons déterminer les conditions dans les-

quelles un tel fait peut se produire, et démontrer le théorème suivant :

THÉORÈME. — *Pour qu'une fonction* φ_1 *appartenant à un groupe* G *d'ordre* r *prenne pour les substitutions d'un groupe* G′ *d'ordre* mr *contenant* G m *valeurs appartenant au même groupe, il faut et il suffit que* G *soit un sous-groupe invariant de* G′.

En effet, en nous reportant au tableau (T) du § précédent, les valeurs $\varphi_1, \varphi_2, \ldots, \varphi_m$ ont pour groupes G, $\Sigma_2^{-1}G\Sigma_2, \ldots, \Sigma_m^{-1}G\Sigma_m$; si ces groupes sont identiques, G est permutable à toute substitution de G′, et est un sous-groupe invariant de G′, et, réciproquement, s'il en est ainsi, les groupes des m valeurs de φ sont identiques.

Les sous-groupes K et H de G_1 remplissaient les conditions précédentes dans les exemples choisis.

Si l'on considère en particulier le cas où G′ est le groupe symétrique, on a, en se reportant aux résultats du § 11, le théorème suivant :

THÉORÈME. — *Les valeurs distinctes que prend une fonction rationnelle de* n *variables pour toutes les substitutions ne peuvent appartenir au même groupe ou s'exprimer rationnellement au moyen de l'une quelconque d'entre elles que dans les deux cas suivants :*

La fonction a deux valeurs appartenant au groupe alterné ;

La fonction a $n\,!$ *valeurs appartenant au groupe réduit à la substitution unité.*

Une seule exception a lieu dans le cas de $n = 4$ *pour les fonctions à six valeurs, telles que* ω_1, *appartenant au groupe* H.

COROLLAIRE. — *Si une fonction rationnelle de* n *variables a un nombre* ρ *de valeurs* > 2 *et* $< n\,!$, *les groupes auxquels appartiennent ces* ρ *valeurs n'ont en commun que la substitution unité, sauf le cas de* $n = 4$ (*).

En effet, si les groupes

$$\Sigma_1^{-1}G\Sigma_1, \qquad \Sigma_2^{-1}G\Sigma_2, \qquad \ldots, \qquad \Sigma_\rho^{-1}G\Sigma_\rho$$

avaient des substitutions communes constituant un groupe H autre que l'unité, ce groupe serait permutable à toute substitution et serait un sous-groupe invariant du groupe symétrique, ce qui est

(*) KRONECKER, *Monatsberichte der Berliner Akademie*, 1879, p. 208.

impossible, sauf pour $n = 4$. Nous avons vu dans ce cas que les groupes G_1, G_2, G_3 ont en commun le groupe H d'ordre 4.

23. Théorème. — *Si une fonction appartenant à un groupe* $G = [S_1, S_2, \ldots, S_r]$ *est telle que les* m *valeurs qu'elle prend pour les substitutions d'un groupe* G' *contenant* G *sont racines d'une équation binome de degré* m, *le groupe* G *est un sous-groupe invariant de* G', *et il existe une substitution* Σ *d'ordre* m *telle que les substitutions de* G' *soient toutes de la forme*

$$S_\alpha \Sigma^\beta \qquad (\alpha = 1, 2, \ldots, r, \quad \beta = 0, 1, \ldots, m-1).$$

En effet, si φ_1 est une fonction appartenant au groupe G telle que les m valeurs $\varphi_1, \varphi_2, \ldots, \varphi_m$ qu'elle prend pour G' soient racines de l'équation

$$\varphi^m - F(\psi_1, f_1, f_2, \ldots, f_n) = 0,$$

où ψ_1 est une fonction du groupe G', ces m valeurs sont de la forme $\varphi_1, \omega\varphi_1, \omega^2\varphi_1, \ldots, \omega^{m-1}\varphi_1$, où ω est une racine primitive de $\omega^m - 1 = 0$. Par suite elles ne diffèrent de l'une d'elles que par un facteur constant, et ont même groupe G; ce groupe est par conséquent un sous-groupe invariant de G'.

De plus si Σ est la substitution qui change φ_1 en $\omega\varphi_1$, les puissances $\Sigma^0, \Sigma^1, \Sigma^2, \ldots, \Sigma^{m-1}$ changent φ_1 respectivement en chacune des m valeurs $\varphi_1, \omega\varphi_1, \omega^2\varphi_1, \ldots, \omega^{m-1}\varphi_1$, et les mr substitutions de G' sont alors de la forme $S_\alpha\Sigma^\beta$, ainsi que cela résulte du tableau T du § 21.

Réciproquement, *en supposant* m *premier absolu, si un groupe* G *d'ordre* r *est sous-groupe invariant d'un groupe* G' *d'ordre* mr, *il existe des fonctions appartenant au groupe* G *dont les* m *valeurs pour les substitutions de* G' *sont racines d'une équation binome de degré* m.

Soit χ_1 une fonction quelconque du groupe G ; par suite de l'hypothèse et de ce que l'on a vu au § précédent, ses m valeurs pour les substitutions de G' appartiennent au même groupe, de sorte que si une substitution Σ de G' change la valeur de χ_1, elle changera en même temps la valeur des $m-1$ autres fonctions; j'appelle χ_2 la fonction dans laquelle Σ transforme χ_1, χ_3 celle dans laquelle Σ transforme χ_2, et ainsi de suite jusqu'à une certaine valeur χ_h que Σ transforme en χ_1.

Je dis que $h = m$; supposons en effet qu'il lui soit inférieur, et soit Σ' une substitution de G' qui change χ_1 en une fonction χ_{h+1} non encore obtenue; la substitution $\Sigma'^{-1}\Sigma\Sigma'$ permutera circulairement les valeurs d'un nouveau cycle de h fonctions χ_{h+1}, $\chi_{h+2}, \ldots, \chi_{2h}$ différentes des premières; si $2h < m$, on continuera de la même manière, de façon que les m fonctions se partagent en cycles d'un même nombre d'éléments. C'est impossible puisque m est premier absolu, par conséquent $h = m$, et Σ permute circulairement les valeurs $\chi_1, \chi_2, \ldots, \chi_m$; de plus Σ est d'ordre m et les puissances $\Sigma^0, \Sigma^1, \ldots, \Sigma^{m-1}$ transforment χ_1 respectivement en $\chi_1, \chi_2, \ldots, \chi_m$, de sorte que les substitutions de G' sont de la forme

$$S_\alpha \Sigma^\beta \qquad (\alpha = 1, 2, \ldots, r, \quad \beta = 0, 1, \ldots, m-1).$$

Cela posé, soit ω une racine primitive de $\omega^m - 1 = 0$, et posons

$$\varphi_1 = \chi_1 + \omega\chi_2 + \ldots + \omega^{m-1}\chi_m.$$

C'est une fonction qui reste invariable pour les substitutions de G; on aura ses valeurs pour celles de G' en lui appliquant les puissances de Σ, ce qui donne

$$\varphi_2 = \chi_2 + \omega\chi_3 + \cdots + \omega^{m-1}\chi_1 = \omega^{-1}\varphi_1,$$

$$\varphi_3 = \chi_3 + \omega\chi_4 + \cdots + \omega^{m-1}\chi_2 = \omega^{-2}\varphi_1,$$

. . . .

$$\varphi_m = \chi_m + \omega\chi_1 + \cdots + \omega^{m-1}\chi_{m-2} = \omega^{-(m-1)}\varphi_1;$$

ce sont des valeurs différentes de la première. Il pourrait arriver pour un choix particulier de χ_1 que φ_1 reste invariable pour certaines substitutions ne faisant pas partie de G', mais on peut toujours prendre pour χ_1 une fonction telle que cela n'ait pas lieu; en prenant par exemple, comme on l'a vu,

$$\chi_1 = (u - \psi_1)(u - \psi_2)\ldots(u - \psi_r),$$

où ψ_1 est la fonction de Galois, $\psi_1, \psi_2, \ldots, \psi_r$ ses valeurs pour le groupe G, on peut donner aux coefficients des valeurs telles que φ_1 varie pour toute substitution n'appartenant pas à ce groupe.

De cette façon on a formé une fonction φ_1 appartenant au groupe G et dont les m valeurs pour G' sont racines d'une équation binome de degré m; toute autre fonction appartenant au même groupe G s'exprimera rationnellement au moyen de celle-là.

24. Corollaire I. — *Si une fonction rationnelle de n variables a plus de deux valeurs pour toutes les substitutions, ses valeurs ne peuvent être les racines d'une équation binome à coefficients symétriques.*

En effet, si une fonction φ_1 à ρ valeurs $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ est telle que ses ρ valeurs soient racines d'une équation binome

$$\varphi^\rho - F(f_1, f_2, \ldots, f_n) = 0,$$

le groupe $G = (S_1, S_2, \ldots, S_r)$ de φ_1 doit être un sous-groupe invariant du groupe symétrique, et de plus il doit exister une substitution Σ d'ordre ρ telle que celles du groupe symétrique soient de la forme $S_\alpha \Sigma^\beta$; or pour $n > 4$ le groupe symétrique n'a pour sous-groupes invariants que le groupe alterné et le groupe réduit à la substitution unité ; au premier appartiennent les fonctions à deux valeurs ; au second les fonctions à $n\,!$ valeurs ; mais aucune n'est racine d'une équation binome de degré $n\,!$, car le groupe symétrique serait composé des puissances d'une substitution Σ d'ordre $n\,!$ et il n'en existe aucune pour $n > 2$ (§ 3).

Pour $n = 4$, outre les deux cas que nous venons de mentionner, peut se présenter celui du groupe H d'ordre 4 qui est sous-groupe invariant du groupe symétrique ; mais il n'existe aucune substitution Σ d'ordre 6 telle que les produits des substitutions de H par les puissances de Σ constituent le groupe symétrique. Il n'y a donc que les fonctions du groupe alterné qui puissent, avec leurs valeurs conjuguées, être racines d'une équation binome à coefficients symétriques ; cette équation est du second degré.

25. Corollaire II. — *Si une fonction rationnelle de n variables, n étant supérieur à 4, appartient à un sous-groupe du groupe alterné, et a m valeurs pour les substitutions de ce groupe, ces valeurs ne peuvent être racines d'une équation binome dont les coefficients appartiennent au groupe alterné.*

Supposons en effet qu'il existe une fonction dont les m valeurs pour les substitutions du groupe alterné soient racines d'une équation binome ; son groupe doit être un sous-groupe invariant du groupe alterné, et se réduire, pour $n > 4$, à la substitution unité, comme on l'a vu au § 11. Le groupe alterné lui-même doit alors se composer des puissances d'une même substitution d'ordre $\frac{n\,!}{2}$; mais on a vu que c'est impossible pour $n > 3$ (§ 3).

Examinons les cas particuliers de $n = 3$ et $n = 4$, auxquels ne s'applique pas le raisonnement précédent.

Pour $n = 3$, le groupe alterné se compose précisément des puissances Σ^0, Σ^1, Σ^2 d'une substitution circulaire d'ordre 3, telle que $\Sigma = (x_1x_2x_3)$; je vais montrer qu'il est possible de former une fonction de Galois dont le cube appartient au groupe alterné et a deux valeurs.

Prenons en effet une fonction de Galois quelconque,

$$\psi_1 = u_1x_1 + u_2x_2 + u_3x_3,$$

et ses valeurs pour le groupe alterné :

$$\psi_1, \qquad \psi_2 = u_1x_2 + u_2x_3 + u_3x_1 \qquad \text{et} \qquad \psi_3 = u_1x_3 + u_2x_1 + u_3x_2;$$

d'après ce que nous avons dit à la fin du § 23, nous devons former, au moyen d'une racine cubique de l'unité, la fonction $\psi_1+\omega\psi_2+\omega^2\psi_3$ dont la valeur est

$$\psi_1 + \omega\psi_2 + \omega^2\psi_3 = (u_1 + \omega^2u_2 + \omega u_3)(x_1 + \omega x_2 + \omega^2x_3);$$

nous pouvons, ce qui ne change pas le résultat, nous limiter à la fonction suivante :

$$\psi_1 = x_1 + \omega x_2 + \omega^2x_3;$$

elle répond à la question, et l'on a, en calculant son cube,

$$\psi_1^3 = \Sigma x_1^3 + 6x_1x_2x_3 - \frac{3}{2}\Sigma x_1^2x_2 - 3\left(\omega + \frac{1}{2}\right)(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$
$$= f_1^3 - \frac{9}{2}f_1f_2 + \frac{27}{2}f_3 - 3\left(\omega + \frac{1}{2}\right)\sqrt{\Delta},$$

où Δ est le discriminant; c'est bien une fonction du groupe alterné.

Pour $n = 4$, il n'existe aucune fonction à 24 valeurs répondant à la question, car il n'existe aucune substitution circulaire d'ordre 12 dont les puissances constituent le groupe alterné; il ne peut s'en trouver que parmi celles qui appartiennent au groupe H d'ordre 4, qui est sous-groupe invariant du groupe alterné. En se reportant au tableau du § 8, on voit que ce dernier groupe est dérivé de H en multiplant ses substitutions par les puissances de la substitution circulaire d'ordre 3 $\Sigma = (x_1x_2x_3)$.

On prendra alors, en posant, comme on l'a déjà fait, $\varphi_1 = x_1x_2 + x_3x_4$, la fonction $\varphi_1 - \varphi_2$ appartenant au groupe H, ses valeurs $\varphi_2 - \varphi_3$ et $\varphi_3 - \varphi_1$ obtenues en effectuant les substitutions Σ et Σ^2, et la

somme

$$\varphi_1 - \varphi_2 + \omega(\varphi_2 - \varphi_3) + \omega^2(\varphi_3 - \varphi_1),$$

où ω est une racine cubique imaginaire de l'unité, ou bien encore

$$z_1 = \varphi_1 + \omega\varphi_2 + \omega^2\varphi_3 = (x_1x_2 + x_3x_4) + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3),$$

qui ne diffère de la première que par un facteur constant ; z_1^3 s'exprime au moyen des fonctions symétriques de $\varphi_1, \varphi_2, \varphi_3$ et de leur discriminant par un calcul identique à celui que l'on a fait pour $n = 3$; on a vu que le discriminant des trois valeurs φ est identique à celui des quatre variables x, par conséquent z_1^3 est une fonction appartenant au groupe alterné.

CHAPITRE V

DES FONCTIONS CYCLIQUES ET MÉTACYCLIQUES DE PLUSIEURS VARIABLES

---

26. Dans ce chapitre nous désignerons pour plus de commodité les n variables par $x_0, x_1, \ldots, x_{n-1}$; supposons-les rangées dans un ordre tel que les indices aillent en croissant, et considérons la substitution circulaire

$$S_1 = (x_0 x_1 \ldots x_{n-1}) ;$$

cette substitution et ses puissances forment un groupe d'ordre n,

$$C_1 = [1, \quad S_1, \quad S_2 = S_1^2, \quad \ldots, \quad S_{n-1} = S_1^{n-1}],$$

appelé groupe cyclique. On peut représenter les substitutions de ce groupe par la notation

$$S_\alpha = | z \quad z + \alpha | \qquad (\text{mod. } n),$$

en signifiant par là que chaque indice z est remplacé par $z + \alpha$, ou par le reste de ce nombre à n.

Si l'on range les variables dans un ordre quelconque, la substitution circulaire

$$S = (x_h x_k x_l \ldots),$$

comprenant dans un seul cycle les n variables, est d'ordre n ; elle définit par ses puissances un groupe qui est analogue au précédent, et en est le transformé par la substitution

$$\Sigma = \begin{pmatrix} x_0 x_1 x_2 \ldots \\ x_h x_k x_l \ldots \end{pmatrix}.$$

Il ne diffère de C_1 que par la notation des variables, et nous l'appellerons encore groupe cyclique. Comme on peut toujours supposer que x_0 soit placé au premier rang dans S, on peut former

autant de substitutions S différentes qu'il y a de permutations des $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$, c'est-à-dire $(n-1)!$; ce sont les transformées de la substitution particulière S_1 par les $N = (n-1)!$ substitutions du groupe symétrique G_0 de

$$x_1, x_2, \ldots, x_{n-1}.$$

Les groupes cycliques qu'elles déterminent sont les transformés $C_1, C_2, \ldots, C_N$ de C_1 par ces substitutions ; nous verrons plus loin qu'ils ne sont pas tous distincts.

Nous appellerons fonction cyclique toute fonction appartenant à l'un des groupes précédents ; il est facile d'en former une appartenant au groupe C_1 par exemple ; désignons par ω une racine primitive de l'équation $x^n - 1 = 0$, et considérons la fonction

$$w_1 = (x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{n-1} x_{n-1})^n = \psi_1^n ;$$

elle reste invariable par les substitutions du groupe, car S_α a pour effet de multiplier la fonction de Galois entre parenthèse ψ_1 par $\omega^{-\alpha}$ et w_1 par $\omega^{-\alpha n} = 1$; réciproquement, si une substitution laisse invariable la fonction w_1, elle a pour effet de multiplier ψ_1 par une racine n^e de l'unité, par exemple par $\omega^{-\alpha}$, et par suite d'augmenter chaque indice de α, comme le fait la substitution S_α du groupe cyclique ; w_1 appartient bien au groupe C_1.

Les fonctions cycliques jouissent de propriétés remarquables et jouent un grand rôle dans la théorie des équations, comme nous le verrons plus loin ; la première de ces propriétés résulte du théorème suivant.

Théorème. — *Chacune des variables est une fonction rationnelle de l'une d'entre elles et d'une fonction cyclique arbitrairement choisies, les coefficients de cette fonction rationnelle étant symétriques.*

Soit, en effet, $\gamma_1(x_0, x_1, \ldots, x_{n-1})$ une fonction cyclique appartenant au groupe C_1 et x_0 une des variables ; le groupe C_1 et celui auquel appartient x_0, qui est le groupe symétrique G_0 des $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$ n'ont en commun que la substitution unité, car il n'existe dans le groupe cyclique que cette substitution laissant x_0 invariable ; par suite la fonction

$$u_0 x_0 + u_1 \gamma_1(x_0, x_1, \ldots, x_{n-1}),$$

où u_0 et u_1 sont arbitraires, est une fonction analogue à la fonction de Galois, au moyen de laquelle s'expriment toutes les autres et en

particulier les variables $x_0, x_1, x_2, \ldots, x_{n-1}$; elles s'expriment ainsi rationnellement au moyen de x_0 et de γ_1, avec des coefficients symétriques par rapport aux n variables.

27. Toute fonction cyclique acquiert pour toutes les substitutions $N = (n-1)!$ valeurs conjuguées satisfaisant à une équation de degré N à coefficients symétriques ; ces valeurs sont toutes des fonctions cycliques, car leurs groupes sont des transformés de C_1, et sont cycliques ; on obtient ces valeurs conjuguées en opérant sur la première les N substitutions du groupe symétrique G_0. Remarquons encore que l'on obtient, comme au § 14, le groupe symétrique en multipliant les substitutions de C_1 par celles de G_0, car toute substitution se ramène d'une seule manière à une substitution du groupe C_1 suivie d'une autre qui laisse x_0 invariable ; il résulte de là que les groupes relatifs aux N valeurs conjuguées sont précisément les groupes cycliques conjugués $C_1, C_2, \ldots, C_N$ du § précédent, c'est-à-dire

$$\Sigma_1^{-1}C_1\Sigma_1, \qquad \Sigma_2^{-1}C_1\Sigma_2, \qquad \ldots, \qquad \Sigma_N^{-1}C_1\Sigma_N,$$

où $\Sigma_1, \Sigma_2, \ldots, \Sigma_N$ sont les $(n-1)!$ substitutions du groupe symétrique de $x_1, \ldots, x_{n-1}$.

Tous ces groupes conjugués n'ont, comme on sait, aucune substitution qui leur soit commune à tous, en dehors de la substitution unité, mais je vais montrer qu'il n'y a parmi eux que $(n-2)!$ groupes distincts, et qu'ils sont respectivement égaux $n-1$ à $n-1$, en supposant toutefois essentiellement que n est un nombre premier.

Je vais chercher pour cela s'il existe une substitution Σ laissant x_0 invariable telle que $\Sigma^{-1}S_1\Sigma$ soit égale à l'une des substitutions S_α ; si

$$\Sigma = \begin{pmatrix} x_0 & x_1 & x_2 & \ldots, & x_{n-1} \\ x_0 & x_{t_1} & x_{t_2} & \ldots, & x_{t_{n-1}} \end{pmatrix}$$

est une telle substitution, on a

$$\Sigma^{-1}S_1\Sigma = (x_0 x_{t_1} x_{t_2} \ldots x_{t_{n-1}}) ;$$

pour qu'elle appartienne au groupe C_1, il faut que $t_{h+1} - t_h$ soit constant et égal à $t_1 - 0 = t_1$, donc que

$$t_2 = 2t_1, \quad t_3 = 3t_1, \quad \ldots, \quad t_{n-1} = (n-1)t_1,$$

par suite que Σ soit de la forme

$$\Sigma = \begin{pmatrix} x_0 & x_1 & x_2 & \ldots, & x_{n-1} \\ x_0 & x_t & x_{2t} & \ldots, & x_{(n-1)t} \end{pmatrix},$$

ce que nous indiquerons par la notation

$$\Sigma = | \, z \quad tz \, | \qquad \text{(mod. } n);$$

de plus, que les restes à n de $t, 2t, \ldots, (n-1)t$ soient les $n-1$ premiers nombres, ce qui a lieu pour toute valeur de t comprise dans la suite $1, 2, \ldots, n-1$, puisque n est premier absolu.

Réciproquement, toute substitution Σ de la forme précédente répond à la question, et est telle que $\Sigma^{-1}C_1\Sigma = C_1$; si l'on prend en effet le nombre t' tel que $tt' \equiv 1$ (mod. n) et si l'on remarque que $\Sigma^{-1}S_1\Sigma = S_t = S_1^t$, on a

$$(\Sigma^{-1}S_1\Sigma)^{t'} = S_1^{tt'} = S_1,$$

de sorte que le groupe $\Sigma^{-1}C_1\Sigma$ contient S_1 et ses puissances et est identique à C_1.

Aux $n-1$ valeurs de t : $1, 2, \ldots, n-1$, correspondent $n-1$ groupes conjugués identiques à C_1 ; d'une manière générale, les N groupes se partagent en $(n-2)!$ séries comprenant chacune $n-1$ groupes identiques. On en conclut que, parmi les $(n-1)!$ fonctions cycliques conjuguées, on peut en choisir $(n-2)!$ particulières telles que les autres en soient des fonctions rationnelles à coefficients symétriques.

28. Toujours en supposant n premier absolu, les produits des substitutions du groupe cyclique C_1 par les substitutions

$$\Sigma_t = | \, z \quad tz \, | \quad \text{(mod. } n) \quad (t = 1, 2, \ldots, n-1)$$

constituent un groupe ; cela tient à ce que

$$\Sigma_t^{-1}S_1\Sigma_t = S_1^t, \qquad \Sigma_t^{-1}S_1^\alpha\Sigma_t = S_1^{t\alpha},$$

d'où, en multipliant en avant par Σ_t, $S_1^\alpha\Sigma_t = \Sigma_t S_1^{t\alpha}$, ou bien $S_1^\alpha\Sigma_t = \Sigma_t S_1^\beta$, α et β étant liés par $t\alpha \equiv \beta$ (mod. n) ; par suite un produit tel que $(S_1^\alpha\Sigma_t)(S_1^{\alpha'}\Sigma_{t'})$ se ramène à la forme $S_1^{\alpha''}\Sigma_{t''}$ et fait partie du même ensemble que les facteurs ; ce groupe, qui comprend $n(n-1)$ substitutions, peut être représenté par la notation

$$M = | \, z \quad az+b \, | \quad \text{(mod. } n) \quad \begin{pmatrix} a = 1, & 2, & \ldots, & n-1 \\ b = 0, & 1, & 2, & \ldots, & n-1 \end{pmatrix}$$

et il s'appelle groupe métacyclique relatif aux n variables $x_0, x_1, \ldots, x_{n-1}$. Toute fonction appartenant à ce groupe s'appelle fonction métacyclique (*) ; il est facile d'en former une particulière de la manière suivante :

Soit g une racine primitive (mod. n) [Voir la note à la fin du volume] ; les restes (mod. n) des $n-1$ puissances $g, g^2, \ldots, g^{n-1}$ sont les $n-1$ premiers nombres ; considérons les fonctions cycliques

$$w_1 = (x_0 + \omega^g x_1 + \omega^{2g} x_2 + \cdots + \omega^{(n-1)g} x_{n-1})^n = \psi_1^n,$$
$$w_2 = (x_0 + \omega^{g^2} x_1 + \omega^{2g^2} x_2 + \cdots + \omega^{(n-1)g^2} x_{n-1})^n = \psi_2^n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$w_{n-1} = (x_0 + \omega^{g^{n-1}} x_1 + \omega^{2g^{n-1}} x_2 + \cdots + \omega^{(n-1)g^{n-1}} x_{n-1})^n = \psi_{n-1}^n,$$

qui appartiennent au groupe C_1 ; elles se transforment les unes dans les autres pour les substitutions du groupe métacyclique ; soit en effet $\Sigma_t = | \, z \;\; tz \, |$ (mod. n) une substitution particulière de ce groupe ; elle transforme w_h en

$$w'_h = (x_0 + \omega^{g^h} x_t + \omega^{2g^h} x_{2t} + \cdots)^n$$

ou, en introduisant le nombre t' tel que $tt' \equiv 1$ (mod. n), et posant $t' = g^k$,

$$w'_h = (x_0 + \omega^{t'g^h} x_1 + \omega^{2t'g^h} x_2 + \cdots)^n = (x_0 + \omega^{g^{h+k}} x_1 + \omega^{2g^{h+k}} x_2 + \cdots)^n = w_{h+k} ;$$

lorsqu'on prend pour h les valeurs $1, 2, \ldots, n-1$, les nombres $h+k$ ont pour restes (mod. n) les $n-1$ premiers nombres dans un ordre quelconque ; par suite les nouvelles valeurs $w'_1, w'_2, \ldots, w_{n-1}$ sont identiques, à l'ordre près, à $w_1, w_2, \ldots, w_{n-1}$. Les substitutions du groupe métacyclique étant composées de celles du groupe C_1 et des substitutions Σ_t, laisseront par suite invariables les fonctions w_1 ou les transformeront les unes dans les autres.

Ce sont les seules qui jouissent de cette propriété, car si une substitution T change w_h en w_k, elle transforme ψ_h en ψ_k, à un multiple près égal à une racine n^e de l'unité ; par exemple en $\omega^l \psi_k$, c'est-à-dire

$$x_0 + \omega^{g^h} x_1 + \omega^{2g^h} x_2 + \cdots$$

en

$$\omega^l x_0 + \omega^{l+g^k} x_1 + \omega^{l+2g^k} x_2 + \cdots ;$$

(*) KRONECKER, *Monatsberichte*, 1879, p. 217.

prenons les deux nombres a et b tels que

$$l + bg^k \equiv 0 \qquad (\text{mod. } n),$$
$$l + (a+b)g^k \equiv g^h \qquad (\text{mod. } n);$$

alors on a

$$ag^k \equiv g^h, \qquad zag^k \equiv zg^h \qquad \text{et} \qquad l + (az+b)g^k \equiv zg^h;$$

par suite, à cause de l'indépendance des variables et de l'inégalité des coefficients, la substitution T a pour effet de transformer $x_0, x_1, x_2, \ldots$ respectivement en $x_b, x_{a+l}, x_{2a+b}, \ldots,$ et est identique à la substitution

$$| \, z \quad az+b \, | \qquad (\text{mod. } n)$$

du groupe métacyclique.

Il résulte de cette propriété de l'ensemble des fonctions cycliques précédentes que la fonction

$$(w - w_1)(w - w_2)\ldots(w - w_{n-1}),$$

où w est une quantité arbitraire non nulle, reste invariable pour les substitutions du groupe métacyclique et pour celles-là seulement, et appartient à ce groupe.

Toute fonction cyclique de $w_1, w_2, \ldots, w_{n-1}$, par exemple la fonction

$$(w_1 + \alpha w_2 + \alpha^2 w_3 + \cdots + \alpha^{n-2} w_{n-1})^{n-1},$$

où α est une racine primitive de l'équation $x^{n-1} - 1 = 0$, appartient au groupe métacyclique ; nous avons vu en effet que toute substitution Σ_t a pour effet de transformer w_h en w_{h+k}, où k est fixe quel que soit h, par suite de laisser invariable la fonction cyclique que nous avons écrite, et on démontre comme précédemment que les substitutions du groupe métacyclique sont les seules possédant cette propriété.

Remarquons que nous venons de former une fonction du groupe C_1,

$$w_1 + \alpha w_2 + \cdots + \alpha^{n-2} w_{n-1},$$

qui est racine d'une équation binome à coefficients appartenant au groupe métacyclique, car sa puissance $(n-1)^e$ appartient à ce groupe ; on vérifie du reste facilement qu'on se trouve placé dans les conditions dont nous avons parlé au § 23 pour qu'il en soit ainsi ; le groupe cyclique C_1 est en effet un sous-groupe invariant particulier du groupe métacyclique M.

29. Nous pouvons encore énoncer un théorème concernant les fonctions métacycliques, et analogue à celui du § 26 :

Théorème. — *Chacune des variables est une fonction rationnelle de deux d'entre elles et d'une fonction métacyclique arbitrairement choisie, les coefficients de cette fonction rationnelle étant symétriques.*

Soit $m(x_0, x_1, \ldots, x_{n-1})$ une fonction métacyclique appartenant au groupe M et x_h, x_k deux quelconques des variables ; il n'existe dans le groupe M aucune substitution autre que l'unité laissant h et k fixes, car si l'on a $ah + b \equiv h$ et $ak + b \equiv k$, on en déduit $a \equiv 1$ et $b \equiv 0 \pmod{n}$; par suite le groupe M et le groupe symétrique des $n-2$ variables autres que x_h et x_k n'ont en commun que la substitution unité, et la fonction

$$u_0 x_h + u_1 x_k + u_2 m(x_0, \quad x_1, \ldots, x_{n-1})$$

est une fonction analogue à la fonction de Galois, au moyen de laquelle s'expriment rationnellement toutes les autres et en particulier les variables ; celles-ci sont donc des fonctions rationnelles de x_h, x_k et m, avec des coefficients symétriques.

Toute fonction métacyclique acquiert pour toutes les substitutions $(n-2)!$ valeurs conjuguées satisfaisant à une équation de degré $(n-2)!$ à coefficients symétriques ; ce sont des fonctions métacycliques, à la notation près des variables ; on les obtient en laissant x_0 et x_1 invariables et effectuant sur les $n-2$ autres variables $x_2, x_3, \ldots, x_{n-1}$ toutes les substitutions possibles dans la fonction donnée appartenant au groupe M ; cela tient à ce fait que les substitutions du groupe M multipliées par celles qui ne changent que $x_2, x_3, \ldots, x_{n-1}$ reproduisent toutes les substitutions possibles des n variables.

30. Nous allons généraliser la notion de fonction cyclique et de groupe de substitutions cycliques, comme l'a indiqué Kronecker dans son mémoire « Sur les Équations abéliennes (*) ».

Nous avons considéré précédemment n variables $x_0, x_1, \ldots, x_{n-1}$ et le groupe d'ordre n formé par la substitution circulaire $S = (x_0 \, x_1 \ldots x_{n-1})$ et ses puissances.

Nous dirons que les fonctions appartenant à ce groupe sont des fonctions cycliques simples des variables, ou à simple entrée.

Prenons maintenant $n = n_1 n_2$ variables affectées chacune de deux indices

(*) Kronecker, *Monatsberichte*, 1877, p. 845.

$$x_{h_1h_2} \quad \begin{pmatrix} h_1 = 0, & 1, & 2, & \ldots & n_1 - 1 \\ h_2 = 0, & 1, & 2, & \ldots & n_2 - 1 \end{pmatrix}$$

et les substitutions circulaires portant sur l'un des indices indépendamment de l'autre; elles forment un groupe composé des substitutions

$$S_1 = (x_{00}\ x_{10}\ x_{20} \ldots x_{n_1-10})(x_{01}\ x_{11}\ x_{21} \ldots x_{n_1-11}) \ldots (x_{0n_2-1}\ x_{1n_2-1} \ldots x_{n_1-1n_2-1}),$$

$$S_2 = (x_{00}\ x_{01}\ x_{02} \ldots x_{0n_2-1})(x_{10}\ x_{11}\ x_{12} \ldots x_{1n_2-1}) \ldots (x_{n_1-10}\ x_{n_1-11} \ldots x_{n_1-1n_2-1}),$$

qui sont respectivement d'ordre n_1 et n_2, de leurs puissances et de leurs produits; comme les substitutions S_1 et S_2 sont échangeables, c'est-à-dire que $S_1S_2 = S_2S_1$, le groupe renferme n_1n_2 substitutions ; on peut le représenter par la notation

$$| z_1 \quad z_1 + 1 | \qquad (\text{mod. } n_1)$$

$$| z_2 \quad z_2 + 1 | \qquad (\text{mod. } n_2);$$

z_1 et z_2 représentant les deux indices. Toute fonction appartenant à ce groupe sera dite une fonction cyclique à deux entrées.

Plus généralement, soient $n = n_1n_2 \ldots n_\nu$ variables affectées chacune de ν indices

$$x_{h_1h_2 \ldots h_\nu} (h_1 = 0, 1, 2, \ldots, n_1 - 1;\ h_2 = 0, 1, \ldots, n_2 - 1;\ h_\nu = 0, 1, \ldots, n_\nu - 1)$$

et les substitutions circulaires d'ordres respectifs $n_1, n_2, \ldots, n_\nu$ relatives à chacun des indices indépendamment des autres,

$$| z_1 \quad z_1 + 1 | \qquad (\text{mod. } n_1),$$

$$| z_2 \quad z_2 + 1 | \qquad (\text{mod. } n_2),$$

$$\cdots\cdots$$

$$| z_\nu \quad z_\nu + 1 | \qquad (\text{mod. } n_\nu);$$

elles sont échangeables et engendrent un groupe d'ordre $n = n_1n_2 \ldots n_\nu$; toute fonction invariable par les substitutions de ce groupe sera dite une fonction cyclique à ν entrées.

31. Le théorème du § 26 s'étend aux fonctions cycliques générales; cela résulte de ce que le groupe cyclique ne renferme aucune substitution autre que l'unité laissant fixe une des variables. Il est facile de former une fonction d'une variable donnée et d'une fonction cyclique qui soit égale à l'une des autres variables; considérons en effet le produit

$$\Phi(x) = \Pi(x - x_{h_1h_2 \ldots h_\nu})$$

étendu à toutes les variables, et la fonction

$$\theta_\alpha(x) = \Sigma x_{h_1 h_2 \ldots h_\alpha+1 \ldots h_\nu} \frac{\Phi(x)}{x - x_{h_1 h_2 \ldots h_\nu}} \cdot \frac{1}{\Phi'(x_{h_1 h_2 \ldots h_\nu})},$$

où la somme est étendue à toutes les combinaisons des indices h; le coefficient de chaque puissance de x est une fonction cyclique s'exprimant rationnellement au moyen d'une fonction cyclique particulière quelconque; d'après la formule de Lagrange, on a, pour toutes les valeurs des indices h,

$$x_{h_1 h_2 \ldots h_\alpha+1 \ldots h_\nu} = \theta_\alpha(x_{h_1 h_2 \ldots h_\alpha \ldots h_\nu}).$$

On aurait de même, en formant une deuxième fonction $\theta_\beta(x)$ analogue à la précédente,

$$x_{h_1 h_2 \ldots h_\beta+1 \ldots h_\nu} = \theta_\beta(x_{h_1 h_2 \ldots h_\beta \ldots h_\nu})$$

etc., de sorte que, en fonction de la variable $x_{00\ldots0}$ par exemple, on aura

$$x_{h_1 h_2 \ldots h_\nu} = \theta_1^{h_1}[\theta_2^{h_2}[\ldots \theta_\nu^{h_\nu}(x_{00\ldots0})]].$$

Il est évident que deux quelconques des fonctions θ ainsi formées jouissent de la propriété

$$\theta_\alpha[\theta_\beta(x_{h_1 \ldots h_\nu})] = \theta_\beta[\theta_\alpha(x_{h_1 \ldots h_\nu})],$$

car le résultat est $x_{h_1 \ldots h_\alpha+1 \ldots h_\beta+1 \ldots h_\nu}$. Nous verrons l'application de ce théorème dans l'étude des équations abéliennes.

CHAPITRE VI

DOMAINE DE RATIONALITÉ. — RÉDUCTIBILITÉ DES FONCTIONS ENTIÈRES (*)

---

32. Étant donnés des paramètres R', R'', R''', ..., que nous supposons indéterminés et indépendants les uns des autres, nous appelons domaine de rationalité l'ensemble de toutes les fonctions rationnelles que l'on peut former au moyen de ces paramètres et des nombres entiers ; nous disons que ces quantités définissent le domaine $(R'R''...)$ et que les fonctions rationnelles précédentes sont des éléments de ce domaine. Toute fonction rationnelle d'un nombre quelconque d'éléments du domaine fait encore partie du même domaine; le domaine le plus simple est formé par les nombres entiers et rationnels, il ne contient plus aucun paramètre.

Soient maintenant x, y, z,... des variables indépendantes ; nous appellerons fonction entière de ces variables dans le domaine $(R'R''...)$ une fonction entière par rapport à x, y, z,... dont les coefficients sont des éléments du domaine, c'est-à-dire des fonctions rationnelles des paramètres.

Toute fonction entière peut se mettre sous la forme du quotient de deux fonctions : l'une entière par rapport aux variables et aux paramètres, avec des coefficients entiers, l'autre entière par rapport aux paramètres seulement, avec des coefficients entiers.

(*) Les considérations qui font l'objet de ce chapitre ont été développées surtout par Kronecker dans sa « Festschrift zum Kummer's Jubilæum » ; consulter aussi son article « Zerlegung der ganzen Grœssen », *Crelle*, t. 94, le mémoire de M. Molk « Sur une notion qui comprend celle de la divisibilité », *Acta Mathematica*, t. 6, et l'« Introduction à la Théorie des Nombres et à l'Algèbre Supérieure » de MM. Borel et Drach.

Le produit de deux fonctions entières dans un domaine donné est une autre fonction entière dans le même domaine. Nous dirons qu'une fonction entière $f(x, y, z, \ldots, R', R'', \ldots)$ est réductible dans le domaine donné si elle est le produit de plusieurs fonctions entières dans le même domaine, irréductible dans le cas contraire ; par exemple dans le domaine des nombres entiers $4x^2 - 9$ est réductible, et $x^2 - 3$ est irréductible.

33. Nous nous proposons de résoudre le problème suivant :

Étant donnée une fonction entière dans un domaine donné de rationalité, chercher si elle est réductible ou non et, dans le premier cas, la décomposer en facteurs irréductibles.

Nous montrerons que l'on peut résoudre ce problème à l'aide d'un nombre limité d'opérations. Nous allons d'abord considérer le cas simple d'une fonction entière d'une seule variable dans le domaine de rationalité formé par les nombres entiers ; on peut toujours mettre la fonction sous la forme

$$\frac{p}{q} f(x) = \frac{p}{q}(a_0 x^n + a_1 x^{n-1} + \cdots + a_n),$$

où $a_0, a_1, \ldots, a_n$ sont des entiers sans diviseur commun, et $\frac{p}{q}$ une fraction irréductible, et l'on a à rechercher si $f(x)$ est réductible ou irréductible, c'est-à-dire admet des diviseurs entiers à coefficients rationnels ou entiers.

Je vais montrer qu'il suffit de se limiter à ce dernier cas, et démontrer le lemme suivant de Gauss :

Si un polynome à coefficients entiers est divisible par un polynome à coefficients rationnels, il est égal au produit de deux polynomes à coefficients entiers.

Supposons que le polynome $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ admette le diviseur $\varphi(x)$ à coefficients rationnels, de façon que

$$f(x) = \varphi(x)\psi(x),$$

où $\psi(x)$ est de même nature que $\varphi(x)$; en mettant en évidence le dénominateur commun aux coefficients de chacun de ces polynomes, on a une identité de la forme

$$f(x) = \frac{\varphi_1(x)}{m} \cdot \frac{\psi_1(x)}{m'},$$

où $\varphi_1(x)$ a ses coefficients entiers, sans diviseur commun avec m, et de même $\psi_1(x)$ a ses coefficients entiers sans diviseur commun avec m' ; je vais montrer que m' divise tous les coefficients de $\varphi_1(x)$ et m tous ceux de $\psi_1(x)$, ou bien, ce qui suffit pour la démonstration, que tout diviseur premier p de m' divise tous les coefficients de $\varphi_1(x)$.

Tous ceux de $\psi_1(x)$ n'étant pas divisibles par p, nous désignerons par $\chi_1(x)$ le reste de la division par p de ce polynome, et nous aurons en chassant les dénominateurs une identité de la forme

$$pf_1(x) = \varphi_1(x)\chi_1(x);$$

comme le coefficient du terme de plus haut degré de $\chi_1(x)$ n'est pas divisible par p, les relations d'identification montrent que p doit diviser tous les coefficients de $\varphi_1(x)$, ce qui était à démontrer ; alors $f(x)$ est égal au produit des deux polynomes $\frac{\varphi_1(x)}{m'}$ et $\frac{\psi_1(x)}{m}$ à coefficients entiers.

34. La question est ainsi ramenée à la recherche des diviseurs à coefficients entiers du polynome $f(x)$, et il suffit de se limiter aux diviseurs dont le degré ne dépasse pas la moitié du degré de $f(x)$.

Si l'on se donne le degré ν d'un diviseur $\varphi(x)$, on peut toujours exprimer ce polynome au moyen de la formule de Lagrange, en fonction de $\nu+1$ entiers, arbitrairement choisis, $x_1, x_2, \ldots, x_{\nu+1}$, par exemple $0, 1, 2, \ldots, \nu$, et de $\nu+1$ quantités arbitraires, $u_1, u_2, \ldots, u_{\nu+1}$, qui représentent les valeurs de $\varphi(x)$ pour

$$x_1, x_2, \ldots, x_{\nu+1};$$

en posant

$$\Phi(x) = (x - x_1)(x - x_2)\ldots(x - x_{\nu+1}),$$

on a

$$\varphi(x) = \sum_1^{\nu+1} u_h \frac{\Phi(x)}{x - x_h} \frac{1}{\Phi'(x_h)}; \tag{1}$$

mais $\varphi(x)$ devant diviser $f(x)$, $\varphi(x_h) = u_h$ est un entier qui doit diviser $f(x_h)$; u_h doit donc être compris parmi les diviseurs entiers du nombre $f(x_h)$, diviseurs qui sont en nombre limité ; on est ainsi amené à décomposer en facteurs chacun des nombres

$$f(x_1), f(x_2), \ldots, f(x_{\nu+1}),$$

et à choisir de toutes les manières possibles les entiers

$$u_1,\ u_2,\ \ldots,\ u_{\nu+1},$$

respectivement parmi les diviseurs de ces nombres ; on a ainsi, en les transportant dans (1), un nombre limité de polynomes $\varphi(x)$; on essayera si ceux d'entre eux qui sont à coefficients entiers divisent effectivement $f(x)$; si aucune division ne réussit, c'est que le polynome donné n'a aucun diviseur de degré ν.

En donnant à ν les valeurs successives $1,\ 2,\ \ldots,$ on verra, par un nombre limité d'opérations portant sur des nombres entiers, si $f(x)$ est irréductible ou a des diviseurs ; ces derniers se trouvent déterminés par cela même.

On peut mettre de cette façon une fonction entière d'une variable dans le domaine des nombres entiers sous la forme

$$\frac{\alpha\beta\ldots}{\alpha'\beta'\ldots}\cdot \mathrm{P}(x).\mathrm{Q}(x)\ldots,$$

où $\alpha,\ \beta,\ \ldots,\ \alpha',\ \beta',\ \ldots$ sont des nombres premiers, $\mathrm{P}(x),\ \mathrm{Q}(x),\ \ldots$ des polynomes à coefficients entiers et sans diviseur.

La décomposition n'est possible que d'une seule manière ; cela résulte de cette propriété des polynomes irréductibles, que l'on démontre comme pour les nombres entiers : si un polynome irréductible divise un produit de plusieurs polynomes, il divise au moins l'un d'eux.

35. Je considère maintenant le cas d'un polynome entier par rapport à q variables $x,\ y,\ z,\ \ldots,$ dont les coefficients appartiennent au domaine défini par les nombres entiers ; en supposant qu'on ait résolu pour $q-1$ variables le problème proposé, on peut employer une marche analogue à la précédente, et utiliser la formule de Lagrange sous la forme (1) ; u_h est alors une fonction de

$$y,\ z,\ \ldots$$

diviseur de $f(x_h,\ y,\ z,\ \ldots)$. On peut aussi ramener immédiatement le cas de q variables à celui d'une seule de la manière suivante :

Soit g un nombre entier supérieur au plus fort exposant de chacune des variables dans le polynome donné ; en posant $y=x^g$, $z=x^{g^2},\ \ldots,$ on transforme la fonction en un polynome entier en x, $\mathrm{F}(x)$. A un terme $x^\alpha y^\beta z^\gamma\ldots$ de f correspond dans F un terme dont l'exposant est $\alpha+\beta g+\gamma g^2+\ldots$; il peut être considéré comme

un nombre écrit avec les chiffres $\alpha, \beta, \ldots$ dans un système de numération de base g, de sorte que les termes de f et F se correspondent d'une manière unique.

Si f est décomposable en un produit de fonctions entières, il en est de même de F ; on est ainsi amené à appliquer à $F(x)$ la méthode exposée plus haut, et à voir si les différentes fonctions en x, y, z qu'on déduit des diviseurs trouvés sont bien des diviseurs de

$$f(x, y, z, \ldots).$$

36. Soit enfin $f(x, y, z, \ldots, R', R'', \ldots)$ un polynome entier par rapport aux variables $x, y, z, \ldots,$ dont les coefficients font partie du domaine $(R', R'', \ldots)$; on peut le mettre sous la forme

$$\frac{\varphi(R', R'', \ldots)}{\psi(R', R'', \ldots)} f(x, y, z, \ldots, R', R'', \ldots),$$

où φ et ψ sont des polynomes entiers par rapport à $R', R'', \ldots$ sans diviseur commun et f un polynome entier par rapport aux variables $x, y, z, \ldots,$ les coefficients étant de même des fonctions entières, à coefficients entiers, des paramètres $R', R'', \ldots,$ sans diviseur commun entier par rapport à ces paramètres. La recherche des diviseurs de f est basée sur les trois lemmes suivants :

Lemme I. — *Si le produit de deux fonctions entières de q variables $x, y, z, \ldots,$ à coefficients entiers, est divisible par une fonction entière de $q-1$ de ces variables, $y, z, \ldots,$ également à coefficients entiers et irréductible, l'une des deux premières fonctions est divisible par la troisième.*

Lemme II. — *Si le produit de deux fonctions entières de q variables, à coefficients entiers, est divisible par une fonction entière des mêmes variables, à coefficients entiers et irréductible, l'une des premières fonctions est divisible par la troisième.*

Lemme III. — *Si une fonction de q variables, à coefficients entiers, est le produit de deux fonctions entières par rapport à l'une de ces variables et rationnelles par rapport aux autres, elle est le produit de deux fonctions entières par rapport à toutes les variables.*

Supposons ces lemmes démontrés dans le cas où les fonctions contiennent respectivement une variable de moins. Pour démontrer le premier, considérons la fonction $g(y, z, \ldots)$, entière par rap-

port à $q-1$ variables et irréductible, divisant le produit

$$\varphi(x, y, z, \ldots)\psi(x, y, z, \ldots) ;$$

ordonnons ces deux polynomes suivant les puissances de x et soient

$$\varphi(x, y, z, \ldots) = a_0(y, z, \ldots)x^m + a_1x^{m-1} + \cdots + a_m,$$

$$\psi(x, y, z, \ldots) = b_0(y, z, \ldots)x^n + b_1x^{n-1} + \cdots b_n.$$

Si tous les coefficients de φ ne sont pas divisibles par g, et si

$$\varphi_1(x, y, z, \ldots)$$

est l'ensemble des termes de φ non divisibles par cette fonction, le produit de $\varphi_1\psi$ doit l'être ; en écrivant que les coefficients du produit sont divisibles par g, et appliquant le deuxième lemme au cas de $q-1$ variables, on voit que $b_0, b_1, \ldots, b_n$ sont tous divisibles par g, ce qui démontre le premier lemme.

En ce qui concerne le second, soit $f(x, y, z, \ldots)$ une fonction entière irréductible des q variables divisant le produit

$$\varphi(x, y, z, \ldots)\psi(x, y, z \ldots).$$

Si φ n'est pas le produit de f par un polynome entier, ordonnons ces deux polynomes par rapport aux puissances décroissantes de x, et divisons φ par f par rapport à cette variable ; la division n'aura pas lieu exactement, même avec des coefficients rationnels en $y, z, \ldots$; en effet, si l'on avait, après réduction des termes du quotient au même dénominateur,

$$\varphi(x, y, z, \ldots) = f(x, y, z, \ldots)\frac{\chi(x, y, z, \ldots)}{\chi_1(y, z, \ldots)},$$

d'où

$$\chi_1(y, z, \ldots)\varphi(x, y, z, \ldots) = f(x, y, z, \ldots)\chi(x, y, z, \ldots),$$

tout facteur irréductible de χ_1 divisant le second membre et ne divisant pas le polynome irréductible f, diviserait χ d'après le premier lemme démontré, et φ serait le produit de f par un polynome entier, contrairement à l'hypothèse.

On peut donc, d'après la théorie du plus grand commun diviseur, trouver deux polynomes φ_1 et f_1 entiers en x, à coefficients rationnels en $y, z, \ldots$, tels que

$$ff_1 + \varphi\varphi_1 = 1,$$

ou bien, en mettant le dénominateur commun en évidence,

$$f(x, y, z, \ldots)f_2(x, y, z, \ldots) + \varphi(x, y, z, \ldots)\varphi_2(x, y, z, \ldots) = g(y, z, \ldots),$$

où f_2, φ_2 et g sont des polynomes entiers ; on en déduit

$$f_2\psi + \frac{\varphi\psi}{f}\varphi_2 = \frac{g\psi}{f};$$

le premier membre est, d'après les hypothèses faites sur le produit $\varphi\psi$, un polynome entier, $h(x, y, z...)$, et l'on a

$$g(y, z, \ldots)\psi(x, y, z, \ldots) = f(x, y, z, \ldots)h(x, y, z, \ldots);$$

d'après le premier lemme démontré, les facteurs irréductibles de g doivent tous diviser h, de sorte que $h = gh_1$; alors $\psi = fh_1$ et f divise ψ, ce qui démontre le deuxième lemme.

Pour vérifier l'exactitude du troisième, soit $f(x, y, z, ...)$ une fonction entière de q variables égale au produit de deux fonctions $\varphi(x, y, z, \ldots)$ et $\psi(x, y, z, \ldots)$, entières par rapport à x et rationnelles par rapport à $y, z, \ldots$; en mettant en évidence les dénominateurs communs, on aura

$$f(x, y, z, \ldots) = \frac{\varphi_1(x, y, z, \ldots)}{\varphi_2(y, z, \ldots)} \times \frac{\psi_1(x, y, z, \ldots)}{\psi_2(y, z, \ldots)},$$

où φ_1 est un polynome entier en x dont les coefficients entiers en $y, z, \ldots$ n'ont aucun diviseur commun avec le polynome entier φ_2, et où il en est de même pour ψ_1 et ψ_2 ; ψ_2 divise φ_1 car, d'après le premier lemme, tout facteur irréductible $p(y, z, ...)$ de ψ_2 divisant le produit $\varphi_1\psi_1$ et étant premier avec ψ_1 divise φ_1, et de même φ_2 divise ψ_1 ; par suite f est le produit de deux polynomes entiers par rapport à toutes les variables.

Les trois lemmes ayant été démontrés dans le cas de $q = 1$ sont ainsi démontrés quel que soit le nombre des variables.

Cela étant posé, si le polynome $f(x, y, z, \ldots, R', R'', \ldots)$ admet des diviseurs entiers par rapport à x, y, z, ... et rationnels par rapport à R', R'', ..., il en admettra d'autres entiers non seulement par rapport aux variables, mais encore par rapport aux paramètres ; on est amené de cette manière à chercher les diviseurs de f entiers par rapport à tous les éléments $x, y, z, \ldots, R', R'' \ldots$, ce que nous savons faire, comme on l'a vu, à l'aide d'un nombre limité d'opérations.

On peut démontrer, en s'appuyant sur les lemmes précédents, que la décomposition ainsi obtenue est unique. Si l'on veut décomposer la fonction

$$\frac{\varphi(R', R'', \ldots)}{\psi(R', R'', \ldots)} f(x, y, z, \ldots, R', R'', \ldots)$$

en fonctions entières en $x, y, z, \ldots$, à coefficients rationnels en $R', R'', \ldots$, on opérera la décomposition des fonctions entières f, φ, ψ en leurs facteurs entiers irréductibles, et l'on attribuera aux diviseurs de f, comme facteurs, des fractions divisant $\frac{\varphi}{\psi}$, et cela d'une manière arbitraire ; nous supposerons désormais que l'on ne considère que des fonctions entières, à coefficients entiers par rapport aux paramètres, ce qui ne change rien aux raisonnements.

37. Soit $f(x, R', R'', \ldots) = 0$ une équation algébrique entière par rapport à x, dont les coefficients sont des éléments du domaine $(R', R'', \ldots)$; nous savons reconnaître si le premier membre est réductible ou non, et trouver ses facteurs irréductibles dans le domaine ; si f est irréductible, nous dirons que l'équation $f = 0$ est irréductible dans le domaine de rationalité; si n est son degré, ses n racines seront n fonctions algébriques du domaine, et nous dirons qu'elles sont conjuguées.

Théorème. — *Si une équation algébrique* $F(x, R', R'' \ldots) = 0$ *a une racine commune avec une équation irréductible* $f(x, R', R'', \ldots) = 0$ *dans le même domaine de rationalité, elle admet toutes les racines de cette seconde équation.*

En effet, les deux polynomes F et f ont un plus grand commun diviseur D que l'on sait déterminer par divisions successives ; si D a un degré inférieur à celui de f, f est décomposable en un produit de facteurs entiers en x, dans le domaine $(R', R'' \ldots)$, et par suite n'est pas irréductible dans ce domaine, contrairement à l'hypothèse, dès lors D est identique à f, et F est égal au produit de f par un polynome entier ; par conséquent, $F = 0$ admet toutes les racines de l'équation irréductible $f = 0$.

Nous appellerons équation générale de degré n une équation de la forme

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n = 0$$

pour laquelle le domaine de rationalité est constitué par les coefficients $c_1, c_2, \ldots, c_n$, supposés indéterminés et indépendants ; ce domaine $(c_1, c_2, \ldots, c_n)$ est identique à celui des fonctions symétriques $f_1, f_2, \ldots, f_n$ des n racines $x_1, x_2, \ldots, x_n$. Si l'on fait varier d'une manière quelconque les paramètres c, les racines

varient, et l'équation générale $f(x) = 0$ jouit précisément de la propriété fondamentale suivante : le système des n variables $c_1, c_2, \ldots, c_n$ est équivalent au système des n autres variables $x_1, x_2, \ldots, x_n$. En effet, à tout système de valeurs des c correspond un système unique de valeurs des x, et réciproquement, et si les unes varient d'une manière continue, il en est de même des autres.

L'équation générale est irréductible dans le domaine des fonctions symétriques ou dans le domaine des coefficients $(c_1, c_2, \ldots, c_n)$: autrement dit, le premier membre $f(x)$ n'est pas décomposable en facteurs entiers en x, à coefficients rationnels par rapport aux coefficients c. En effet, si cela avait lieu on pourrait, comme on l'a vu précédemment, mettre $f(x)$ sous la forme du produit de deux polynomes entiers non seulement par rapport à x, mais encore par rapport à $c_1, c_2, \ldots, c_n$, avec des coefficients entiers ; comme $f(x)$ contient linéairement les coefficients c, l'un des deux facteurs les renfermerait aussi linéairement, tandis que l'autre en serait indépendant et aurait comme coefficients des nombres entiers. Supposons donc que l'on ait

$$f(x) = \varphi(x)\psi(x),$$

où $\varphi(x)$ est un polynome entier à coefficients numériques et entiers ; donnons à x une valeur entière arbitraire x_0 ; nous pouvons ensuite donner à $c_1, c_2, \ldots, c_n$ des valeurs entières telles que $f(x_0)$ ne soit pas divisible par le nombre entier $\varphi(x_0)$; comme $\varphi(x_0)$ et $\psi(x_0)$ sont des nombres entiers, on voit que l'égalité précédente est impossible, et par conséquent que $f(x)$ est irréductible.

Toute équation dont les coefficients font partie d'un autre domaine que celui des fonctions symétriques des racines est une équation particulière ; par exemple une équation à coefficients numériques, entiers ou fractionnaires, est une équation particulière dont le domaine de rationalité se réduit à celui des nombres entiers ; en général, les fonctions symétriques, ou bien les coefficients d'une équation particulière sont des éléments du domaine de rationalité, mais ils sont fixes ou sont reliés par des relations, ce qui fait qu'il peut exister pour une telle équation des relations entre les racines.

Une équation particulière peut être réductible dans le domaine de rationalité choisi ; si l'on prend par exemple comme domaine de rationalité celui qui est défini par les racines $(x_1, x_2, \ldots, x_n)$, les

coefficients s'expriment comme on sait au moyen de ces éléments, et le polynome est décomposable en facteurs linéaires dans le domaine sous la forme

$$f(x) = (x - x_1)(x - x_2)\dots(x - x_n).$$

Pour une équation particulière, les coefficients ne font pas toujours partie du domaine de rationalité, mais renferment quelquefois des fonctions algébriques des éléments de ce domaine, ou encore, comme cas particulier, des racines d'équations entières à coefficients entiers.

Si $R_1, R_2, \dots$ sont de telles fonctions algébriques de $R', R'', \dots$, on dit que les coefficients font partie du domaine de rationalité, $(R', R'', \dots)$, auquel on adjoint les fonctions algébriques $R_1, R_2, \dots$ des éléments de ce domaine.

Par exemple, l'équation

$$x^3 - x + 2\sqrt{3} = 0$$

a ses coefficients faisant partie du domaine des nombres entiers, auquel on adjoint une racine de l'équation $R^2 - 3 = 0$.

38. Nous nous proposons de chercher si une fonction entière d'une variable (on peut ramener à ce cas celui de plusieurs variables) est réductible ou non dans le domaine général $(R_1, R_2, \dots, R', R'', \dots)$, et de résoudre en même temps le problème suivant : chercher si une fonction dont les coefficients font partie du domaine $(R', R'', \dots)$ et qui est irréductible dans ce domaine est réductible ou non lorsqu'on adjoint à ce domaine des fonctions algébriques $R_1, R_2, \dots$; les deux questions sont identiques.

Remarquons d'abord qu'on peut remplacer l'adjonction de plusieurs fonctions algébriques par celle d'une seule convenablement choisie ; soient $R_1, R_2, \dots$ des fonctions définies par les équations irréductibles

$$\varphi(R_1, R', R'', \dots) = 0, \qquad \psi(R_2, R', R'', \dots) = 0.$$

Prenons la somme

$$u_1 R_1 + u_2 R_2 + \cdots,$$

où $u_1, u_2, \dots$ sont des constantes laissées arbitraires ; le produit

$$\Pi(z - u_1 R_1 - u_2 R_2 - \cdots),$$

étendu à tous les systèmes de valeurs de $R_1, R_2, \dots$, est une fonc-

tion symétrique de ces quantités, et est une fonction $\Phi(z, u_1, u_2, \ldots, R', R'', \ldots)$ du domaine $(R', R'', \ldots)$; décomposons-la en ses facteurs irréductibles par rapport à $z, u_1, u_2, \ldots$ dans le domaine précédent et désignons par $\Phi_1(z, u_1, \ldots)$ celui de ces facteurs divisible par $z - u_1R_1 - u_2R_2 - \cdots$; en posant $u_1 = v_1 + \alpha_1$, $u_2 = v_2 + \alpha_2, \ldots$, où $\alpha_1, \alpha_2, \ldots$ sont des nombres rationnels particuliers, on obtient la fonction

$$\Phi_1(z, \quad v_1 + \alpha_1, \quad v_2 + \alpha_2, \ldots \quad R', R'', \ldots),$$

qui s'annule pour $z = (v_1 + \alpha_1)R_1 + (v_2 + \alpha_2)R_2 + \cdots$; en remplaçant d'autre part $u_1, u_2, \ldots$ par $v_1, v_2, \ldots$ et z par $z - \alpha_1R_1 - \alpha_2R_2 - \ldots$, on obtient la deuxième fonction

$$\Phi_1(z - \alpha_1R_1 - \alpha_2R_2 - \cdots, \quad v_1, v_2, \ldots, R', R'', \ldots),$$

qui s'annule pour

$$z - \alpha_1R_1 - \alpha_2R_2 - \ldots = v_1R_1 + v_2R_2 + \cdots ;$$

ces deux fonctions ont en commun le facteur

$$z - (v_1 + \alpha_1)R_1 - (v_2 + \alpha_2)R_2 - \cdots$$

et n'en ont pas d'autre si $\alpha_1, \alpha_2, \ldots$ sont choisis de façon que l'équation $\Phi_1(z, \alpha_1, \alpha_2, \ldots, R', R'', \ldots) = 0$ ait ses racines distinctes ; par l'opération donnant le plus grand commun diviseur, on aura le diviseur commun, et par suite en l'annulant on obtiendra

$$(v_1R_1 + v_2R_2 + \cdots) + (\alpha_1R_1 + \alpha_2R_2 + \cdots)$$

en fonction rationnelle de $v_1, v_2, \ldots, \alpha_1, \alpha_2, \ldots$ et de

$$R = \alpha_1R_1 + \alpha_2R_2 + \cdots,$$

qui est racine de l'équation

$$\Phi_1(R, \alpha_1, \alpha_2, \ldots, R', R'', \ldots) = 0 ;$$

il suffit de donner, à la fin du calcul, des valeurs numériques rationnelles particulières aux indéterminées $v_1, v_2, \ldots$ pour avoir $R_1, R_2, \ldots$ exprimés rationnellement au moyen de la seule fonction algébrique R.

On verrait plus généralement que l'adjonction de fonctions algébriques liées entre elles et aux paramètres $R', R'', \ldots$ par des équations quelconques se ramène à l'adjonction d'une seule fonction des paramètres.

39. Cela posé, soit $f(x, R, R', R'', \ldots)$ une fonction entière en x, dont les coefficients font partie du domaine défini par $R', R'', \ldots$

auquel on adjoint une fonction algébrique R, liée aux paramètres par une équation irréductible $\varphi(R, R', R'', \ldots) = 0$, de degré n ; je désigne ses racines par $R_1, R_2, \ldots, R_n$. Comme R peut ne pas entrer dans f, je remplace x par $z + uR$, et je forme le produit

$$\Pi_k f(z + uR_k, R_k, R', R'', \ldots),$$

étendu à toutes les racines R_k ; c'est une fonction symétrique de ces racines, et par suite une fonction entière de z et u dans le domaine $(R', R'', \ldots)$; je la décompose en ses facteurs irréductibles dans ce domaine ; soit

$$\Pi f(z + uR_k, R_k, R', R'', \ldots) = \Phi_1(z)\Phi_2(z)\ldots\Phi_\nu(z).$$

Une fonction telle que $\Phi_1(z)$ a un diviseur commun avec $f(z + uR_1, R_1, \ldots)$ par exemple ; je forme le plus grand commun diviseur de ces deux fonctions, soit $\theta_1(z, R_1)$; on sait qu'il leur est relié par des identités de la forme

$$\theta_1(z, R_1) = \Phi_1(z)\psi(z, R_1) + f(z + uR_1, R_1, \ldots)\chi(z, R_1),$$

$$\Phi_1(z) = \theta_1(z, R_1)\psi_1(z, R_1),$$

$$f(z + uR_1, R_1, \ldots) = \theta_1(z, R_1)\chi_1(z, R_1).$$

Ces identités ayant lieu pour une racine de l'équation irréductible qui définit R_1, ont lieu pour toutes les autres, d'où l'on conclut que $\theta_1(z, R_k)$ est le plus grand commun diviseur de $\Phi_1(z)$ et de $f(z + uR_k, R_k, \ldots)$.

On a du reste

$$\Phi_1(z) = \theta_1(z, R_1)\theta_1(z, R_2)\ldots\theta_1(z, R_n);$$

en effet, le second membre est un diviseur de Φ_1, car les facteurs qui le composent divisent Φ_1, et l'on verrait facilement qu'ils sont premiers entre eux ; d'autre part les identités précédentes donnent, en formant le produit des valeurs de $\theta_1(z, R_1)$, $\theta_1(z, R_2)$, ... tirées de la première et des analogues, une identité de la forme

$$\Pi\theta_1(z, R_k) = \Phi_1(z)H(z) + \Pi f(z + uR_k, R_k, \ldots)K(z),$$

où le produit qui entre dans le second membre est égal à $\Phi_1(z)\Phi_2(z)\ldots$; on en conclut que le produit des fonctions θ est divisible par $\Phi_1(z)$; il lui est par suite identique.

Si l'on répète le même calcul avec $\Phi_2(z), \ldots, \Phi_\nu(z)$, on a de nouveaux diviseurs $\theta_2(z, R_k), \ldots, \theta_\nu(z, R_k)$; on a alors, quel que soit k,

$$f(z + uR_k, R_k, \ldots) = \theta_1(z, R_k)\theta_2(z, R_k)\ldots\theta_\nu(z, R_k);$$

il suffit de remplacer ensuite z par $x - uR_k$ pour avoir une décomposition de $f(x)$ en ν facteurs; il sont irréductibles, car si θ_1 par exemple était décomposable en plusieurs facteurs, $\Phi_1(z)$ qui est le produit $\Pi_k\theta_1(z, R_k)$ serait décomposable dans le domaine $(R', R'', \ldots)$.

Par exemple la fonction

$$f(x, \sqrt{3}) = x^3 - x + 2\sqrt{3}$$

est réductible dans le domaine formé par les nombres entiers auxquels on adjoint une racine de l'équation $R^2 - 3 = 0$; en posant $R_1 = \sqrt{3}$, $R_2 = -R_1$ et $u = 0$, on a

$$f(x, R_1)f(x, R_2) = x^6 - 2x^4 + x^2 - 12 = (x^2 - 3)(x^4 + x^2 + 4).$$

Les diviseurs communs de ces facteurs avec $x^3 - x + 2R_1$ sont respectivement $x + R_1$ et $x^2 - R_1x + 2$, de sorte que

$$f(x, R_1) = (x + R_1)(x^2 - R_1x + 2) = (x + \sqrt{3})(x^2 - x\sqrt{3} + 2).$$

40. Remarque. — Les questions que nous venons de traiter sont purement algébriques, et ne s'appliquent pas immédiatement à la géométrie ; nous avons étudié la réductibilité des fonctions entières dans un domaine donné à l'avance, et nous avons remarqué qu'une fonction irréductible dans un domaine peut le devenir dans un autre; par exemple une fonction d'une seule variable est toujours réductible en facteurs linéaires lorsqu'on adjoint au domaine de rationalité les fonctions algébriques définies par la fonction égalée à zéro. Pour les fonctions de plusieurs variables, il n'en est plus de même ; une telle fonction peut rester irréductible quelles que soient les quantités adjointes au domaine de rationalité.

En géométrie, on dit qu'une courbe ou une surface représentée par une équation $f(x, y, z, \ldots, R, R' R'', \ldots) = 0$ est réductible si le premier membre admet des diviseurs entiers par rapport aux variables, avec des coefficients faisant partie de domaines quelconques, irréductible dans le cas contraire.

La méthode ordinairement suivie pour voir si une fonction est réductible dans ce sens plus général consiste à essayer la division par une fonction de degré moindre, à coefficients indéterminés, et à chercher les relations auxquelles doivent satisfaire ces coefficients pour que la division soit possible. La théorie générale de l'élimination montre si ces relations sont compatibles ; elle nous apprend de plus qu'il suffit d'adjoindre des fonctions algébriques des éléments du domaine donné primitivement, en nombre limité, pour effectuer la réduction de la fonction lorsque celle-ci est réductible ; elle nous donne non seulement ces fonctions algébriques, mais encore les diviseurs de la fonction.

CHAPITRE VII

DES FONCTIONS RATIONNELLES DES RACINES D'UNE ÉQUATION. — RÉSOLVANTES. — GROUPE D'UNE ÉQUATION ALGÉBRIQUE.

41. Dans les chapitres III et IV, nous avons établi la théorie des fonctions rationnelles de plusieurs variables indépendantes, et montré la relation qui existe entre ces fonctions et les groupes de substitutions. Nous allons maintenant considérer les fonctions de variables généralement non indépendantes, ou de quantités numériquement déterminées ; nous supposerons, ce qui ne nuit en rien à la généralité, et est même nécessaire pour la suite, que les quantités données $x_1, x_2, \ldots, x_n$ sont les racines d'une équation algébrique

$$(1) \qquad f(x, \mathrm{R}, \mathrm{R}', \mathrm{R}'', \ldots) = 0,$$

de degré n, dont les coefficients font partie d'un domaine de rationalité défini par les paramètres $\mathrm{R}', \mathrm{R}'', \ldots,$ auxquels on adjoint dans certains cas une fonction algébrique R de ces paramètres.

Nous ne supposons pas nécessairement l'équation (1) irréductible ; nous admettons cependant dans tout ce qui suit qu'elle n'a pas de racine multiple, c'est-à-dire que le polynome f n'a pas de diviseur commun avec sa dérivée.

Une fonction rationnelle des racines, qu'on peut supposer mise sous la forme du quotient d'une fonction entière par une fonction symétrique (§ 16), appartient algébriquement à un groupe G d'ordre r, en ce sens que pour les substitutions de ce groupe et pour celles-là seulement la fonction donnée $\varphi(x_1, x_2, \ldots, x_n)$ ne change pas de forme algébrique par rapport à $x_1, x_2, \ldots, x_n$; mais il peut se faire

que, pour une autre substitution telle que Σ n'appartenant pas au groupe G, φ reprenne la même valeur numérique, ou la même valeur fonction algébrique des paramètres R, R', R'', ... qui définissent le domaine de rationalité. Nous dirons pour simplifier que φ ne change pas sa valeur numérique dans le domaine considéré; cela a lieu alors pour toutes les substitutions $G\Sigma$, et, plus généralement, les substitutions laissant invariable la valeur numérique de φ forment un groupe G' contenant G comme sous-groupe ; on reconnaît que G' est un groupe plus général que G à ce que l'équation qui a pour racines les $\rho = \frac{n!}{r}$ valeurs algébriques de φ a des racines multiples dont l'une est égale à φ; si φ est racine d'ordre m, l'ordre de G' est égal à mr.

Par exemple, considérons l'équation bicarrée

$$x^4 + px^2 + q = 0$$

dont les racines x_1, x_2, x_3, x_4 sont supposées telles que l'on ait $x_2 = -x_1$, $x_4 = -x_3$; la fonction $\varphi_1 = x_1 + x_2$ appartient algébriquement au groupe

$$G = [1, (x_1x_2), (x_3x_4), (x_1x_2)(x_3x_4)],$$

mais reste numériquement invariable pour $\Sigma = (x_1x_3)(x_2x_4)$ et pour les produits des substitutions de G par Σ, constituant avec G un groupe d'ordre 8 ; cela tient à ce que $x_1 + x_2 = x_3 + x_4 = 0$ et que l'équation qui a pour racines les six valeurs algébriques de φ_1 a une racine double égale à zéro.

42. Théorème. — *Il est toujours possible de former une fonction des n racines d'une équation ayant, pour toutes les substitutions, $n!$ valeurs distinctes numériquement dans le domaine de rationalité.*

Prenons la fonction

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n$$

et ses valeurs ψ_1, ψ_2, ... pour les $n!$ substitutions ; formons toutes les différences possibles de ces valeurs deux à deux ; il est possible de choisir les coefficients u de façon qu'aucune ne soit nulle ; en effet, ordonnons chacune d'elles suivant les paramètres $u_1, u_2, \ldots, u_n$, sous la forme

$$\psi_\alpha - \psi_\beta = u_1(x_{\alpha_1} - x_{\beta_1}) + u_2(x_{\alpha_2} - x_{\beta_2}) + \cdots + u_n(x_{\alpha_n} - x_{\beta_n}).$$

Toutes les différences $x_\alpha - x_\beta$ entrant dans le second membre de l'égalité précédente ne sont pas nulles, puisque les racines sont inégales ; prenons toutes les fonctions $\psi_\alpha - \psi_\beta$ ne renfermant que u_1 et indépendantes de $u_2, \ldots, u_n$; elles ne sont pas nulles, quelle que soit la valeur attribuée à u_1 ; prenons ensuite celles qui renferment u_1 et u_2 ; ayant choisi arbitrairement u_1, on pourra exclure les valeurs de u_2 qui les annuleraient, et choisir le second paramètre u_2 de façon qu'aucune ne soit nulle , en considérant ensuite celles qui renferment u_1, u_2 et u_3, on pourra choisir u_3 pour qu'elles ne soient pas nulles, et ainsi de suite ; de cette façon les $n!$ valeurs de ψ_1 seront numériquement distinctes.

Théorème. — *Il est toujours possible de former une fonction des n racines d'une équation, invariable algébriquement pour les substitutions d'un groupe G d'ordre r, et dont les $\rho = \frac{n!}{r}$ valeurs algébriquement distinctes pour toutes les substitutions le soient aussi numériquement dans le domaine de rationalité.*

Soient $\psi_1, \psi_2, \ldots, \psi_r$ les valeurs de la fonction de Galois que nous venons de déterminer, pour les substitutions $S_1, S_2, \ldots, S_r$ du groupe G ; elles sont algébriquement et numériquement distinctes ; formons le produit

$$\varphi_1 = (u - \psi_1)(u - \psi_2)\ldots(u - \psi_r);$$

il appartient algébriquement au groupe G et a ρ valeurs algébriquement distinctes ; soient

$$\varphi_\alpha = (u - \psi_{\alpha_1})(u - \psi_{\alpha_2})\ldots(u - \psi_{\alpha_r}) \quad \text{et} \quad \varphi_\beta = (u - \psi_{\beta_1})(u - \psi_{\beta_2})\ldots(u - \psi_{\beta_r})$$

deux de ces ρ valeurs ; elles ne sont pas numériquement identiques quel que soit u, car sinon les fonctions ψ_α et ψ_β seraient respectivement égales à l'ordre près, et φ_α serait algébriquement égal à φ_β, ce qui est impossible ; on pourra donc exclure les valeurs de u satisfaisant à l'équation non identique $\varphi_\alpha - \varphi_\beta = 0$ et à toutes les autres analogues et donner dès lors à u une valeur pour laquelle les ρ valeurs soient distinctes numériquement.

Corollaire. — *Au moyen d'une fonction appartenant au groupe G et dont les valeurs algébriquement distinctes le sont aussi numériquement, on peut exprimer rationnellement toute autre fonction apparte-*

nant algébriquement au même groupe ou à un autre contenant le premier.

Il suffit en effet de reprendre le raisonnement du § 17, et d'exprimer la fonction ψ_1 que l'on veut calculer au moyen de la fonction donnée φ_1 en se servant de la formule de Lagrange ; le polynome

$$\Psi(z) = \sum_h \psi_h \frac{\Phi(z)}{z - \varphi_h} \frac{1}{\Phi'(\varphi_h)}$$

donne ψ_h quand on remplace z par φ_h ; le dénominateur commun est le produit $\Pi\Phi'(\varphi_h)$, et il n'est pas nul puisque l'équation $\Phi(z) = 0$ a ses racines inégales.

Lagrange, dans son célèbre mémoire sur la résolution des équations (*), a examiné le cas où l'on donne une fonction quelconque φ_1 des racines appartenant algébriquement au groupe G, et où l'on veut calculer une autre fonction appartenant algébriquement au même groupe ; si les ρ valeurs de φ_1 ne sont pas numériquement distinctes, la méthode précédente est illusoire ; il faut dans ce cas résoudre une équation d'ordre plus ou moins élevé, comme l'a montré Lagrange dans son mémoire. Nous allons cependant démontrer l'important théorème suivant :

43. THÉORÈME. — *Si une fonction φ_1 est numériquement invariable pour les substitutions d'un groupe G, toute autre fonction ψ_1 numériquement invariable pour les substitutions du même groupe ou d'un autre le contenant s'exprime rationnellement au moyen de la première.*

Soit φ_1 la fonction donnée appartenant numériquement au groupe G, mais algébriquement à un autre groupe G_1 qui ne peut être que G ou un sous-groupe de G ; soit de même ψ_1 la fonction que l'on veut calculer, appartenant numériquement à G et algébriquement à un sous-groupe G_2 de G ; soit H le groupe commun à G_1 et G_2 ; si r est l'ordre de H, et $\rho = \frac{n!}{r}$, on peut mettre les $n!$ substitutions du groupe symétrique sous la forme d'un tableau de la forme

$$H\Sigma_1,\ H\Sigma_2,\ \ldots,\ H\Sigma_\rho,$$

où $\Sigma_1, \Sigma_2, \ldots, \Sigma_\rho$ sont convenablement choisies (§ 6 et 14).

(*) Le Mémoire de LAGRANGE fait partie des *Mémoires de l'Académie de Berlin*, 1770 et 1771 ; la partie relative à la question actuelle est reproduite dans l'*Algèbre supérieure* de SERRET, t. II, p. 433.

Les ρ valeurs de φ_1 pour $\Sigma_1, \Sigma_2, \ldots, \Sigma_\rho$ ne sont pas généralement distinctes numériquement ; soient $\varphi_1, \varphi_2, \ldots, \varphi_s$ celles qui le sont ; on pourra toujours former l'équation à coefficients symétriques ayant pour racines les valeurs algébriquement distinctes de φ_1, et en déduire, par la méthode des racines égales, une équation

$$\Phi(z) = (z - \varphi_1)(z - \varphi_2)\ldots(z - \varphi_s) = 0$$

ayant comme racines simples $\varphi_1, \varphi_2, \ldots, \varphi_3$; ses coefficients seront rationnellement exprimables dans le domaine.

De même les ρ valeurs de ψ_1 ne sont pas distinctes numériquement en général, mais par hypothèse toute substitution conservant à φ_1 sa valeur numérique jouira de la même propriété relativement à ψ_1, sans que la réciproque soit nécessairement vraie. Supposons, pour fixer les idées, que parmi les ρ valeurs de φ_1 en existent m numériquement égales à φ_1.

Considérons la fonction

$$\Psi(z) = \sum \psi_h \cdot \frac{\Phi(z)}{z - \varphi_h} \cdot \frac{1}{\Phi'(\varphi_h)},$$

où la somme est étendue aux ρ valeurs que prennent simultanément φ_1 et ψ_1 pour les substitutions $\Sigma_1, \Sigma_2, \ldots, \Sigma_\rho$; elle est composée de ρ termes qui ne sont pas tous distincts en général ; d'après les hypothèses faites, m d'entre eux sont relatifs à φ_1 et ont tous ψ_1 comme coefficient, de sorte que la fonction peut s'écrire

$$\Psi(z) = m\psi_1 \cdot \frac{\Phi(z)}{z - \varphi_1} \cdot \frac{1}{\Phi'(\varphi_1)} + \Sigma\psi_h \cdot \frac{\Phi(z)}{z - \varphi_h} \cdot \frac{1}{\Phi'(\varphi_h)},$$

la somme indiquée au second membre étant étendue aux valeurs de φ autres que φ_1.

$\Psi(z)$ est, dans tous les cas, une fonction symétrique des n racines $x_1, x_2, \ldots, x_n$, car elle ne change pas de valeur algébrique pour une substitution quelconque ; elle s'exprime rationnellement au moyen des coefficients de l'équation donnée, et son dénominateur, qui est le produit

$$\Phi'(\varphi_1).\Phi'(\varphi_2)\ldots\Phi'(\varphi_s),$$

n'est pas nul, puisque $\varphi_1, \varphi_2, \ldots, \varphi_s$ sont racines simples de $\Phi(z) = 0$; ce dénominateur est du reste le discriminant de $\Phi(z)$.

Soit

$$\Psi(z) = A_1 z^{s-1} + A_2 z^{s-2} + \cdots + A_s$$

la fonction ainsi obtenue ; lorsqu'on y remplace z par φ_1, elle prend la valeur $m\psi_1$, de sorte que l'on a

$$m\psi_1 = A_1\varphi_1^{s-1} + A_2\varphi_1^{s-2} + \cdots + A_s\,;$$

ψ_1 est ainsi exprimé au moyen de φ_1 par un polynome entier à coefficients symétriques.

On peut encore raisonner de la manière suivante :

Effectuons sur la fonction $\psi_1\varphi_1^\lambda$ les substitutions $\Sigma_1, \Sigma_2, \ldots, \Sigma_\rho$, et formons la somme des résultats ; c'est une fonction algébriquement symétrique, et par suite rationnellement exprimable ; si nous ordonnons la somme suivant les valeurs distinctes $\varphi_1, \varphi_2, \ldots, \varphi_s$, nous aurons

$$m\psi_1\varphi_1^\lambda + \varphi_2^\lambda(\psi_2' + \psi_2'' + \cdots) + \varphi_3^\lambda(\psi_3' + \psi_3'' + \cdots) + \cdots + \varphi_s^\lambda(\psi_s' + \psi_s'' + \cdots)$$
$$= F_\lambda(R, R', R'', \ldots),$$

où $\psi_2', \psi_2'', \ldots$ sont des valeurs de ψ_1 distinctes ou non, de même ψ_3', ψ_3'', etc. Donnons à λ les valeurs $0, 1, 2, \ldots, s-1$; nous aurons s équations linéaires par rapport à $m\psi_1$, $\psi_2' + \psi_2'' + \cdots$, $\psi_3' + \psi_3'', \ldots$; le déterminant Δ des coefficients est le déterminant de Van der Mond relatif à $\varphi_1, \varphi_2, \ldots, \varphi_s$ et n'est pas nul ; on aura ainsi en particulier

$$m\psi_1 = \frac{\Delta_1}{\Delta} = \frac{\Delta_1\Delta}{\Delta^2},$$

où Δ_1 est le déterminant fourni par la méthode connue de résolution ; sous la dernière forme, $\Delta_1\Delta$ est une fonction symétrique entière de $\varphi_2, \varphi_3, \ldots, \varphi_s$, car

$$\Delta_1\Delta = \begin{vmatrix} F_0 & 1 & 1 & \ldots & 1 \\ F_1 & \varphi_2 & \varphi_3 & \ldots & \varphi_s \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ F_{s-1} & \varphi_2^{s-1} & \varphi_3^{s-1} & \ldots & \varphi_s^{s-1} \end{vmatrix} \times \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \varphi_1 & \varphi_2 & \ldots & \varphi_s \\ \cdot & \cdot & \cdot & \cdot \\ \varphi_1^{s-1} & \varphi_2^{s-1} & \ldots & \varphi_s^{s-1} \end{vmatrix}$$

et s'exprime d'une manière entière au moyen des coefficients de l'équation

$$\frac{\Phi(z)}{z - \varphi_1} = 0,$$

donc d'une manière entière au moyen de φ_1 ; Δ^2 est une fonction symétrique qui n'est autre que le discriminant de $\Phi(z)$ et il n'est pas nul. La proposition se trouve ainsi démontrée.

Comme cas particulier de ce théorème, nous avons le corollaire suivant :

Corollaire. — *Si une fonction des racines d'une équation est numériquement invariable pour toutes les substitutions, elle s'exprime rationnellement au moyen des coefficients de l'équation.*

Il suffit en effet de prendre pour ψ_1 la fonction donnée et pour φ_1 une fonction algébriquement symétrique quelconque ou même l'unité. Si H est le groupe auquel appartient algébriquement la fonction ψ_1 et si r est l'ordre de ce groupe, on aura $s = 1$ et $m = \rho = \frac{n\,!}{r}$, de sorte que

$$\rho\psi_1\varphi_1 = F(R, R', R'', \ldots).$$

On peut encore dire que la somme des valeurs algébriquement distinctes de ψ_1, qui est ici égale à $\rho\psi_1$, est une fonction symétrique des racines et s'exprime rationnellement.

44. En choisissant une fonction de Galois dont les $n\,!$ valeurs soient numériquement distinctes, on a une fonction au moyen de laquelle toute fonction des racines, et en particulier les racines elles-mêmes s'expriment rationnellement, comme nous l'avons dit au § 20.

Il résulte de là que si l'on connaît la valeur d'une telle fonction des racines, on peut déterminer celle des racines elles-mêmes, et l'on a résolu l'équation ; il suffit ainsi, pour résoudre une équation de degré n, et trouver ses n racines, de calculer une seule racine d'une équation de degré $n\,!$, dont les coefficients sont rationnellement connus au moyen de ceux de l'équation donnée ; cette équation auxiliaire de degré $n\,!$ s'appelle équation résolvante de Galois.

Nous appellerons en général résolvante une équation satisfaite par les différentes valeurs d'une fonction déterminée des racines de l'équation donnée, et dont la résolution sert à simplifier celle de cette équation.

La recherche d'une racine de la résolvante de Galois ne complique pas le problème de la détermination des n racines de l'équation donnée, et lui est équivalente ; du reste, pour trouver ces dernières, il faut calculer une racine d'une équation de degré n, puis une

racine d'une équation de degré $n-1$ déduite de la première, et ainsi de suite, et le produit des degrés de ces équations successives est égal à $n\,!$

45. Une autre notion fondamentale introduite par Galois dans le théorie des équations est celle de groupe d'une équation donnée.

Soit

$$(2)\quad f(x,\ \mathrm{R},\ \mathrm{R}',\ \mathrm{R}'',\ldots) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n = 0$$

une équation de degré n dont les coefficients sont des fonctions rationnelles des éléments d'un domaine $(\mathrm{R},\ \mathrm{R}',\ \mathrm{R}'',\ldots)$ et dont les racines sont $x_1,\ x_2,\ldots,\ x_n$. Formons une fonction de Galois

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n$$

ayant des valeurs numériques distinctes pour toutes les substitutions, et l'équation résolvante

$$\Psi(z) = (z-\psi_1)(z-\psi_2)\ldots(z-\psi_{n!}) = 0.$$

Le premier membre est une fonction symétrique des racines x et s'exprime rationnellement dans le domaine ; décomposons-le en ses facteurs irréductibles dans ce domaine, et soit

$$\Psi(z) = \Psi_1(z)\Psi_2(z)\ldots$$

cette décomposition ; supposons que $\Psi_1(z)$ soit le facteur contenant $z-\psi_1$, et que l'on ait

$$\Psi_1(z) = (z-\psi_1)(z-\psi_2)\ldots(z-\psi_r)\,;$$

les fonctions $\psi_1,\ \psi_2,\ldots,\ \psi_r$ se déduisent de ψ_1 par des substitutions que nous désignerons par $\mathrm{S}_1=1,\ \mathrm{S}_2,\ldots,\ \mathrm{S}_r$, effectuées sur les racines ; je dis qu'elles forment un groupe ; en effet, si l'on effectue l'une des substitutions précédentes, telle que S_α, les fonctions $\psi_1, \psi_2,\ldots, \psi_r$ se changent respectivement en des valeurs $\psi'_1,\ \psi'_2,\ldots,\ \psi'_r$; mais le polynome $\Psi_1(z)$ est une fonction des racines qui reste invariable, ainsi que ses coefficients : par suite les nouvelles valeurs des ψ sont, à l'ordre près, identiques aux premières ; si l'on effectue alors successivement deux substitutions $\mathrm{S}_\alpha,\ \mathrm{S}_\beta,\ \psi_1$ sera changé en une des r valeurs $\psi_1,\ \psi_2,\ldots,\ \psi_r$, de sorte que le produit $\mathrm{S}_\alpha\mathrm{S}_\beta$ est une des substitutions de l'ensemble $(\mathrm{S}_1\mathrm{S}_2\ldots\mathrm{S}_r)$; celles-ci forment bien un groupe.

Toute fonction des racines numériquement invariable par les substitutions de ce groupe s'exprime rationnellement au moyen des

éléments du domaine de rationalité. En effet, si $\varphi_1(x_1, x_2, \ldots, x_n)$ est une telle fonction, on peut l'exprimer rationnellement au moyen de la fonction ψ_1 de Galois ; soit $\varphi_1(x_1, \ldots, x_n) = F(\psi_1)$. Effectuons sur $x_1, x_2, \ldots, x_n$ les r substitutions du groupe ; le premier membre φ_1 reste numériquement invariable dans le domaine, et le second devient $F(\psi_2), \ldots, F(\psi_r)$, de sorte que

$$\varphi_1 = F(\psi_1) = F(\psi_2) = \cdots = F(\psi_r) = \frac{1}{r}[F(\psi_1) + F(\psi_2) + \cdots];$$

la parenthèse étant symétrique par rapport à $\psi_1, \psi_2, \ldots, \psi_r$ s'exprime rationnellement au moyen des coefficients de $\Psi_1(z)$, par suite φ_1 a une valeur rationnelle dans le domaine.

Il est évident que si une fonction $\varphi_1(x_1, x_2, \ldots, x_n)$ reste algébriquement invariable par les substitutions du groupe, elle est aussi numériquement invariable dans le domaine, et s'exprime rationnellement.

Réciproquement, toute fonction des racines rationnellement exprimable dans le domaine reste numériquement invariable pour les substitutions du groupe précédent.

En effet, soit $\varphi_1(x_1, x_2, \ldots, x_n) = f(R, R', R'', \ldots)$ une fonction rationnellement exprimable ; exprimons le premier membre au moyen de la fonction ψ_1 de Galois ; si $\varphi_1 = F(\psi_1)$, on aura une équation de la forme

$$F(\psi_1) = f(R, R', R'', \ldots);$$

comme elle admet l'une des racines de l'équation irréductible $\Psi_1(z) = 0$, elle est satisfaite par toutes les autres, de sorte que l'on a, pour chacune d'elles,

$$F(\psi_\alpha) = f(R, R', R'', \ldots) = \varphi_1(x_1, x_2, \ldots, x_n).$$

On voit que la fonction φ_1 conserve la même valeur lorsqu'on remplace ψ_1 par une des valeurs $\psi_2, \ldots, \psi_r$, et par suite reste numériquement invariable pour les substitutions du groupe. On peut dès lors énoncer le théorème suivant (*) :

THÉORÈME. — *Etant donnée une équation* $f(x, R, R', R'', \ldots)$ *dont les racines sont inégales, et dont les coefficients font partie d'un domaine* $(R, R', R'', \ldots)$, *il existe entre les racines un groupe de substitutions*

(*) C. JORDAN, *Traité des Substitutions*, p. 257 ; SERRET, *Algèbre supérieure*, t. II, p. 639.

tel que toute fonction des racines dont les substitutions de ce groupe n'altèrent pas la valeur numérique dans le domaine soit rationnellement exprimable, et réciproquement. Ce groupe est appelé le groupe de l'équation.

46. Pour le déterminer pratiquement, nous considérerons la fonction de Galois

$$\psi_1 = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n,$$

où $u_1, u_2, \ldots, u_n$ sont laissés à dessein indéterminés, et l'équation résolvante

$$\Psi(z) = \Pi[z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n] = 0,$$

où le produit est étendu aux $n!$ substitutions ; si le facteur irréductible $\Psi_1(z)$ qui s'annule pour $z = \psi_1$ est $(z-\psi_1)(z-\psi_2)\ldots(z-\psi_r)$, c'est-à-dire

$$\Psi_1(z) = \Pi_\alpha[z - u_1 x_{\alpha_1} - u_2 x_{\alpha_2} - \cdots - u_n x_{\alpha_n}], \qquad \alpha = 1, 2, \ldots, r,$$

c'est une fonction entière de $z, u_1, u_2, \ldots, u_n$ à coefficients rationnels dans le domaine ; je dis qu'elle appartient, par rapport aux indéterminées $u_1, u_2, \ldots, u_n$, à un groupe identique au groupe G de l'équation.

En effet, la fonction

$$\psi_\alpha = u_1 x_{\alpha_1} + u_2 x_{\alpha_2} + \cdots + u_n x_{\alpha_n},$$

dérivée de ψ_1 par la substitution S_α, peut encore s'écrire, en l'ordonnant par rapport à $x_1, x_2, \ldots, x_n$,

$$\psi_\alpha = u_{\beta_1} x_1 + u_{\beta_2} x_2 + \cdots + u_{\beta_n} x_n,$$

où $(u_{\beta_1}, u_{\beta_2}, \ldots, u_{\beta_n})$ se déduisent de $(u_1, u_2, \ldots, u_n)$ par la substitution $S_\beta = S_\alpha^{-1}$. On obtiendra donc tous les facteurs de $\Psi_1(z)$ en laissant dans $z - \psi_1$ les quantités $x_1, x_2, \ldots, x_n$ fixes et effectuant sur les paramètres $u_1, u_2, \ldots, u_n$ les substitutions $S_1^{-1}, S_2^{-1}, \ldots, S_r^{-1}$, c'est-à-dire toutes les substitutions du groupe G lui-même, prises dans un autre ordre ; on voit ainsi que la fonction entière Ψ_1 des indéterminées $u_1, u_2, \ldots, u_n$ reste algébriquement invariable lorsqu'on effectue sur ces quantités les substitutions d'un groupe identique à celui de l'équation.

Ce sont du reste les seules jouissant de cette propriété ; supposons en effet que Ψ_1 reste invariable pour une substitution S_β effectuée sur $u_1, u_2, \ldots, u_n$; elle le sera alors lorsqu'on laissera ces

paramètres fixes et qu'on effectuera sur $x_1, x_2, \ldots, x_n$ la substitution inverse S_β^{-1} ; comme Ψ_1 est une fonction des racines rationnellement exprimable, S_β^{-1} et par suite S_β appartiennent au groupe G de l'équation.

Pour avoir ce groupe, on aura donc à chercher, parmi les $n\,!$ substitutions, celles qui laisseront algébriquement invariable la fonction $\Psi_1(z, u_1, u_2, \ldots, u_n)$ lorsqu'on les effectuera sur les indéterminées $u_1, u_2, \ldots, u_n$.

En réalité, il reste encore une indétermination dans le problème ; on ne peut distinguer, parmi les facteurs irréductibles de $\Psi(z)$, celui qui admet comme facteur $z - \psi_1$, mais cette indétermination tient à la nature des choses, et est due à ce fait que l'on peut attribuer d'une manière arbitraire les indices $1, 2, \ldots, n$ aux n racines d'une équation. Supposons que la décomposition de $\Psi(z)$ donne

$$\Psi(z) = \Psi_1(z)^{\mu_1}\Psi_2(z)^{\mu_2}\ldots\Psi_\rho(z)^{\mu_\rho}\,;$$

je dis que les facteurs sont du même degré, et affectés du même exposant, égal à l'unité ; en effet, les racines $\psi_1, \psi_2, \ldots, \psi_{n!}$ de $\Psi(z) = 0$ étant toutes distinctes, cette équation n'a pas de racines égales, et les exposants $\mu_1, \mu_2, \ldots, \mu_\rho$ doivent être égaux à l'unité. Soit en outre

$$\Psi_1(z) = (z - u_1x_1 - u_2x_2 \ldots - u_nx_n)(z - u_1x_{2_1} - \ldots)\ldots$$

et Σ une substitution n'appartenant pas au groupe G, transformant $z - \psi_1$ en un facteur $z - \psi_\sigma = z - u_1x_{\sigma_1} - u_2x_{\sigma_2} - \ldots - u_nx_{\sigma_n}$ de $\Psi_2(z)$; à la substitution Σ effectuée sur les x correspond une substitution Σ^{-1} effectuée sur les indéterminées u ; elle transforme $\Psi_1(z)$ en un polynome Ψ_σ entier en z, rationnel dans le domaine donné, et irréductible, car, s'il ne l'était pas, $\Psi_1(z)$ qui s'en déduit par la substitution Σ effectuée sur les quantités u serait réductible contrairement à l'hypothèse. Ce polynome Ψ_σ a de plus un facteur commun $z - \psi_\sigma$ avec $\Psi_2(z)$ qui est irréductible, et par conséquent lui est identique. En répétant ce raisonnement, on voit que les facteurs irréductibles sont du même degré, et se déduisent du premier par des substitutions $\Sigma_2, \Sigma_3, \ldots, \Sigma_\rho$ effectuées sur les x, ou les substitutions inverses sur les u ; on obtient ainsi, au moyen des r facteurs de la forme $z - \psi_1$ de $\Psi_1(z)$, ρr facteurs distincts, et comme les $n\,!$ valeurs de ψ_1 sont différentes, on a $\rho r = n\,!$.

Les groupes déduits des facteurs de $\Psi(z)$ sont respectivement

$$G, \qquad \Sigma_2^{-1}G\Sigma_2, \qquad \Sigma_3^{-1}G\Sigma_3, \ldots, \qquad \Sigma_\rho^{-1}G\Sigma_\rho$$

et sont semblables ; ils sont identiques, au choix près des indices, d'après ce qu'on a vu au § 7, et l'on peut prendre l'un quelconque d'entre eux comme groupe de l'équation.

Chacun des facteurs irréductibles de $\Psi(z)$, égalé à zéro, fournit une équation résolvante dont chaque racine est une fonction de Galois à n ! valeurs ; on peut appeler l'une quelconque de ces équations une résolvante de Galois, et la connaissance d'une seule racine de l'une d'elles entraîne celle des racines $x_1, x_2, \ldots, x_n$ elles-mêmes, c'est-à-dire fournit la résolution de l'équation proposée.

Le procédé de calcul que nous avons indiqué à la fin du § 20 est encore applicable ici. Soit $\Psi_\alpha(z)$ un facteur irréductible de $\Psi(z)$; c'est un polynome entier par rapport à $z, u_1, u_2, \ldots, u_n$, dont les coefficients font partie du domaine de rationalité ; il s'annule identiquement lorsqu'on remplace z par

$$\psi_\alpha = u_{\alpha_1}x_1 + u_{\alpha_2}x_2 + \cdots + u_{\alpha_n}x_n,$$

par exemple, lorsqu'on tient compte des relations qui existent entre les racines x et les coefficients de l'équation. Si l'on prend sa dérivée par rapport à l'une des indéterminées u, elle s'annulera pour $z = \psi_\alpha$, de sorte que les relations

$$x_k \frac{\partial \Psi_\alpha}{\partial z} + \frac{\partial \Psi_\alpha}{\partial u_{\alpha_k}} = 0 \qquad (k = 1, 2, \ldots, n)$$

seront des identités lorsqu'on remplacera z par ψ_α et donneront les valeurs des n racines $x_1, x_2, \ldots, x_n$ en fonction de ψ_α.

On voit de cette façon que la résolution d'une équation de degré n dont le groupe est d'ordre r revient à la détermination d'une seule racine d'une équation résolvante de degré r.

47. Le groupe de l'équation générale est le groupe symétrique ; en effet, s'il en était autrement, et si le groupe de l'équation

$$(3) \qquad f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n = 0$$

était un groupe particulier G, on pourrait former une fonction φ_1 des racines numériquement invariable pour les substitutions de G et variable pour toute autre, rationnellement exprimable, et satis-

faisant alors à une identité de la forme

$$\varphi_1(x_1, x_2, \ldots, x_n) = f(c_1, c_2, \ldots, c_n);$$

or le second membre, lorsqu'on y remplace les coefficients par leurs valeurs en fonction des racines, est symétrique par rapport à $x_1, x_2, \ldots, x_n$ que l'on peut considérer comme variables indépendantes, tandis que le premier membre ne l'est pas; il y a donc impossibilité que le groupe G soit autre que le groupe symétrique.

Lorsque le groupe G d'une équation n'est pas le groupe symétrique, cette équation est spéciale; il existe au moins une fonction des racines appartenant au groupe, non identiquement nulle algébriquement, et rationnellement exprimable, de sorte qu'il existe entre les racines et les éléments du domaine de rationalité au moins une relation de la forme

$$\varphi_1(x_1, x_2, \ldots, x_n) = f(R, R', R'', \ldots).$$

On peut en former d'autres, en choisissant des fonctions numériquement invariables pour le groupe G ou pour un groupe contenant ce dernier, mais toutes ces relations sont caractérisées par le groupe de l'équation et sont contenues implicitement dans l'équation résolvante de Galois. Prenons en effet une telle équation résolvante, par exemple $\Psi_1(z) = 0$; le premier membre est, comme nous l'avons dit, une fonction de $u_1, u_2, \ldots, u_n$ identiquement nulle lorsqu'on remplace z par

$$\psi_1 = u_1x_1 + u_2x_2 + \cdots + u_nx_n;$$

si, après cette substitution, on l'ordonne suivant les puissances des indéterminées u, les coefficients des différents termes seront nuls. Ces coefficients sont du reste des fonctions des racines invariables par les substitutions du groupe et, en les annulant, on obtient des relations entre les racines et les paramètres R, R′, R″, ... du domaine de rationalité.

On peut dire que toutes les relations ainsi obtenues sont contenues dans l'équation unique

$$\Psi_1(u_1x_1 + u_2x_2 + \cdots + u_nx_n) = 0.$$

Je vais montrer inversement que toute relation existant entre les racines est une conséquence de celles dont nous venons de parler; supposons en effet que l'on connaisse *a priori* une relation entre les racines et les éléments du domaine de rationalité

$$f(x_1, x_2, \ldots, x_n, R, R', R'', \ldots) = 0;$$

le premier membre, qui est numériquement égal à zéro, et par conséquent rationnellement exprimable, appartient au groupe de l'équation, d'après le théorème fondamental ; de plus, si l'on remplace $x_1, x_2, \ldots, x_n$ par leurs valeurs en fonction de ψ_1, elle se transforme en une relation

$$F(\psi_1, R, R', R'', \ldots) = 0.$$

Cette équation, ayant une racine commune avec l'équation irréductible $\Psi_1(z) = 0$, a son premier membre divisible par $\Psi_1(\psi_1)$, et chaque facteur irréductible de F est identique à Ψ_1 ; par suite F est égal à une certaine puissance de Ψ_1, et la relation $F(\psi_1) = 0$ est une conséquence de la relation $\Psi_1(\psi_1) = 0$, ainsi que nous l'avions annoncé.

On voit facilement que, dans le cas où le groupe de l'équation est le groupe symétrique, les coefficients des différents termes de la fonction $\Psi(u_1x_1 + u_2x_2 + \cdots + u_nx_n)$ ordonnée suivant les puissances des indéterminées u sont tous des fonctions symétriques des racines, et les relations obtenues dans ce cas sont les relations connues existant entre les coefficients de l'équation et ces fonctions symétriques.

On voit par suite que si l'on connaît les relations distinctes qui existent entre les racines et les éléments du domaine de rationalité, on peut trouver le groupe de l'équation en cherchant les substitutions pour lesquelles ces relations restent numériquement vérifiées.

Ainsi, par exemple, considérons l'équation bicarrée

$$x^4 + px^2 + q = 0,$$

dont les racines sont x_1, $x_2 = -x_1$, x_3 et $x_4 = -x_3$; je dis que le groupe de cette équation est le groupe G_1 du § 12

$$G_1 = [1,\ (x_1x_2),\ (x_3x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3),$$
$$(x_1x_4x_2x_3),\ (x_1x_3x_2x_4)].$$

Par la première méthode, je forme la fonction de Galois

$$\psi_1 = u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = (u_1 - u_2)x_1 + (u_3 - u_4)x_3$$

et l'équation résolvante de Galois ; le facteur relatif au groupe G_1

$$\Psi_1(z) = (z - \psi_1)(z - \psi_2)\ldots(z - \psi_8)$$

est rationnellement exprimable, car c'est une fonction symétrique

de x_1^2 et x_3^2; il est du reste facile à calculer, et est égal à

$$z^8 - 2z^6q[(u_1 - u_2)^2 + (u_3 - u_4)^2] + \cdots;$$

on vérifie que les substitutions du groupe G_1 effectuées sur les u, le laissent invariable. Par la seconde méthode, les relations entre les racines sont

$$x_1 + x_2 = 0, \qquad x_3 + x_4 = 0,$$

et elles restent numériquement invariables pour les substitutions de G_1.

On peut remarquer à ce propos que toute relation entre les racines en entraîne une autre entre les coefficients $c_1, c_2, \ldots, c_n$ de l'équation mise sous la forme (2), car si une telle relation est par exemple $\varphi(x_1, x_2, \ldots, x_n) = 0$, et si l'on effectue le produit des valeurs de φ pour les substitutions qui changent sa forme algébrique, on a une fonction symétrique exprimable au moyen des coefficients et égale à zéro. Réciproquement, toute relation $F(c_1, c_2, \ldots, c_n) = 0$ est une relation entre les racines en remplaçant les coefficients par leurs expressions en $x_1, x_2, \ldots, x_n$; cette relation peut se décomposer en plusieurs autres en général.

Par exemple dans le cas précédent, les coefficients satisfont aux conditions $c_1 = 0$, $c_3 = 0$, qui donnent $x_1 + x_2 = -(x_3 + x_4)$ et $x_1x_2(x_3 + x_4) + x_3x_4(x_1 + x_2) = 0$, d'où $(x_1 + x_2)(x_1x_2 - x_3x_4) = 0$; l'hypothèse $x_1 + x_2 = 0$ donne $x_3 + x_4 = 0$; la seconde, $x_1x_2 = x_3x_4$, jointe à $x_1 + x_2 = -(x_3 + x_4)$, indique que les deux premières racines sont égales et de signes contraires aux deux autres, c'est-à-dire que $x_1 + x_3 = 0$, $x_2 + x_4 = 0$; on obtient toujours le même groupe pour l'équation, au choix près des indices.

48. Nous montrerons plus loin le parti que Galois a tiré de la notion de groupe d'une équation spéciale pour l'étude des équations résolubles; nous voulons pour le moment indiquer la propriété fondamentale suivante :

Considérons une équation $f(x, R, R', R'', \ldots) = 0$ irréductible dans le domaine $(R, R', R'', \ldots)$ et ayant un groupe G. Je dis que ce groupe jouit de la propriété qu'il existe au moins une substitution remplaçant un élément quelconque x_h par un autre x_k arbi-

trairement choisi ; on exprime ce fait en disant que le groupe est transitif (*).

Supposons, en effet, qu'il ne soit pas transitif; il existera alors au moins un groupe d'éléments $x_1, x_2, \ldots, x_\alpha$ en nombre $< n$, tel que toutes les substitutions de G les laissent invariables, ou les permutent entre eux, mais non avec les autres ; s'il en est ainsi, les fonctions symétriques de ces α éléments appartiennent au groupe G et le produit $\varphi(x) = (x - x_1)(x - x_2)\ldots(x - x_\alpha)$ est rationnellement exprimable, par suite f n'est pas irréductible, contrairement à l'hypothèse.

Réciproquement, toute équation dont le groupe est transitif est irréductible ; supposons qu'elle ne le soit pas, et que

$$\varphi(x) = (x - x_1)(x - x_2)\ldots(x - x_\alpha)$$

soit un facteur rationnel de f ; aucune substitution du groupe ne pourra permuter l'un des éléments $(x_1, x_2, \ldots, x_\alpha)$ avec un des autres tel que $x_{\alpha+1}$ et le groupe ne sera pas transitif ; si, en effet, x_1 par exemple est remplacé par $x_{\alpha+1}$ pour une substitution, $\varphi(x)$ ne reste pas invariable pour toutes les substitutions de G et n'est pas rationnellement exprimable. On peut donc énoncer le résultat suivant :

Théorème. — *Toute équation irréductible a son groupe transitif, et réciproquement.*

Ainsi par exemple considérons une équation de degré n telle qu'entre ses racines existe l'unique relation $x_1 + x_2 = 0$; le groupe de cette équation est d'ordre $2(n-2)!$ et se compose des substitutions 1, (x_1x_2) combinées avec celles qui portent sur $x_3, x_4, \ldots, x_n$; il n'est pas transitif et l'équation est réductible. On pourra calculer x_1x_2 au moyen de la formule de Lagrange en fonction de $x_1 + x_2$, car ces deux fonctions ont le même groupe algébrique, et leurs valeurs algébriquement distinctes sont également distinctes en valeur numérique, puisqu'il n'existe aucune autre relation particulière entre les racines que celle qui était donnée ; on formera ainsi en fonction rationnelle des quantités données les coefficients de l'équation

$$x^2 - (x_1 + x_2)x + x_1x_2 = 0,$$

(*) L'étude des groupes transitifs a fait depuis Cauchy l'objet de nombreuses recherches que l'on trouve résumées dans le traité de M. Jordan.

ayant pour racines x_1 et x_2, et on aura de cette façon décomposé l'équation en deux autres de degrés 2 et $n-2$.

49. Nous démontrerons de la même manière la propriété suivante des équations résolvantes relatives à l'équation générale.

Étant donnée l'équation générale de degré n,

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n = 0,$$

toute fonction entière ou rationnelle des racines appartenant à un groupe d'ordre r a pour toutes les substitutions $\rho = \frac{n\,!}{r}$ valeurs algébriquement et numériquement distinctes, racines d'une équation de degré ρ à coefficients fonctions symétriques des racines, par suite fonctions rationnelles des coefficients $c_1, c_2, \ldots, c_n$; je vais montrer que cette équation de degré ρ est irréductible dans le domaine de rationalité $(c_1, c_2, \ldots, c_n)$.

De même si une fonction φ_1 appartient à un groupe G d'ordre r, sous-groupe d'un groupe G' d'ordre mr auquel appartient une fonction ψ_1, les m valeurs $\varphi_1, \varphi_2, \ldots, \varphi_m$ de φ_1 pour les substitutions de G' sont racines d'une équation de degré m à coefficients rationnels par rapport à $c_1, c_2, \ldots, c_n$, et ψ_1; je dis que cette équation est irréductible dans le domaine $(c_1, c_2, \ldots, c_n, \psi_1)$.

Je démontrerai seulement la deuxième de ces propositions, d'où découle la première ; on a vu au § 21 que les substitutions du groupe G' se partagent en m lignes de la forme

$$G\Sigma_1, \qquad G\Sigma_2, \qquad \ldots, \qquad G\Sigma_m,$$

celles de la ligne $G\Sigma_\alpha$ transformant φ_1 en φ_α. Supposons que l'équation de degré m ayant pour racines $\varphi_1, \varphi_2, \ldots, \varphi_m$ soit réductible et que le premier membre admette un facteur

$$(z-\varphi_1)(z-\varphi_2)\ldots(z-\varphi_\alpha)$$

à coefficients rationnels en $c_1, c_2, \ldots, c_n$ et ψ_1; ce facteur ne changera pas pour les substitutions du groupe G', quelle que soit la valeur attribuée à z; or la substitution $\Sigma_{\alpha+1}$ de ce groupe transforme au moins φ_1 en $\varphi_{\alpha+1}$ et ne peut laisser invariable, quel que soit z, le facteur précédent, puisque les m valeurs de φ_1 sont distinctes; il y a donc contradiction, et l'équation est irréductible, comme nous voulions le démontrer.

CHAPITRE VIII

DES ÉQUATIONS DU DEUXIÈME, DU TROISIÈME ET DU QUATRIÈME DEGRÉ. — RECHERCHES DE LAGRANGE

---

50. L'équation générale du deuxième degré,

$$x^2 + c_1 x + c_2 = 0,$$

a un groupe d'ordre deux, $G = [1, (x_1 x_2)]$, et le groupe alterné se réduit à la seule substitution unité ; la fonction de Galois $u_1 x_1 + u_2 x_2$ et les racines elles-mêmes appartiennent au groupe alterné, et s'expriment rationnellement au moyen d'une fonction alternée quelconque.

La fonction $x_1 - x_2$ est une telle fonction dont le carré est symétrique, et n'est autre que le discriminant ; on a ainsi :

$$x_1 - x_2 = \sqrt{\Delta} = \sqrt{c_1^2 - 4c_2},$$

$$x_1 + x_2 = -c_1,$$

$$2x_1 = -c_1 + \sqrt{c_1^2 - 4c_2}, \qquad 2x_2 = -c_1 - \sqrt{c_1^2 - 4c_2}.$$

51. L'équation générale du troisième degré,

$$x^3 + c_1 x^2 + c_2 x + c_3 = 0,$$

a un groupe symétrique d'ordre six, de sorte que la fonction de Galois est racine d'une équation du 6e degré, mais on peut la déterminer au moyen d'autres résolvantes. On aura d'abord une fonction alternée en résolvant une équation du second degré ; en particulier la fonction

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

a deux valeurs égales et de signes contraires, et est égale à la racine

carrée du discriminant ; soit

$$(x_1-x_2)(x_2-x_3)(x_3-x_1) = \sqrt{\Delta} = \sqrt{-(4c_2^3+27c_3^2)+18c_1c_2c_3+c_1^2c_2^2-4c_1^3c_3}$$

cette fonction alternée ; toute autre fonction à deux valeurs s'exprime rationnellement au moyen de la précédente, qui appartient au groupe alterné

$$[1, (x_1x_2x_3), (x_1x_3x_2)].$$

La fonction de Galois $u_1x_1 + u_2x_2 + u_3x_3$ a trois valeurs pour les substitutions de ce groupe, et dépend d'une équation du troisième degré dont les coefficients sont des fonctions à deux valeurs ; cette équation sera une équation binome si l'on prend en particulier la fonction

$$(1) \qquad \psi_1 = x_1 + \omega x_2 + \omega^2 x_3,$$

où ω est une racine cubique imaginaire de l'unité ; comme on l'a vu au § 25, on a, en remplaçant les fonctions symétriques f_1, f_2, f_3 par $-c_1, c_2$ et $-c_3$,

$$(2) \qquad \psi_1^3 = -c_1^3 + \frac{9}{2}c_1c_2 - \frac{27}{2}c_3 - 3\left(\omega + \frac{1}{2}\right)\sqrt{\Delta}.$$

Si l'on prend pour ω la valeur $\dfrac{-1+\sqrt{-3}}{2}$, et qu'on adjoigne au domaine de rationalité ω ou, ce qui revient au même, $\sqrt{-3}$, et de plus $\sqrt{\Delta}$, on a

$$(3) \quad \psi_1^3 = \frac{1}{2}\left[-2c_1^3 + 9c_1c_2 - 27c_3 - 3\sqrt{-3}\sqrt{\Delta}\right] = \frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right],$$

S_1 étant une fonction symétrique.

Il suffit d'avoir une seule racine de cette équation, que nous représenterons par

$$\psi_1 = \sqrt[3]{\frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right]},$$

pour avoir les autres et les racines de l'équation ; nous avons vu en effet au § 20 que l'on a en fonction de ψ_1

$$(4) \qquad x_1 = \frac{\psi_1^2 - c_1\psi_1 + c_1^2 - 3c_2}{3\psi_1},$$

$$x_2 = \frac{\omega\psi_1^2 - \omega^2 c_1\psi_1 + c_1^2 - 3c_2}{3\omega^2\psi_1}, \qquad x_3 = \frac{\omega^2\psi_1^2 - \omega c_1\psi_1 + c_1^2 - 3c_2}{3\omega\psi_1}.$$

Quel que soit le signe que l'on prenne devant $\sqrt{\Delta}$ et la racine de l'équation binome donnant ψ_1 que l'on choisisse, on obtient le

même résultat pour les trois racines, à l'ordre près. En effet, changer le signe de $\sqrt{\Delta}$ revient à effectuer dans la fonction alternée $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ une transposition telle que $(x_1 x_2)$; changer la racine ψ_1 en $\omega\psi_1$ ou $\omega^2\psi_1$ revient à effectuer sur la fonction ψ_1 une des substitutions du groupe alterné ; le résultat est donc le même que si l'on effectuait sur la suite des trois racines x_1, x_2, x_3 une substitution quelconque, ce qui revient à changer simplement la notation de leurs indices.

Une autre méthode employée pour trouver les trois racines consiste à calculer une racine de l'équation (2) et une de l'équation analogue obtenue en changeant le signe de $\sqrt{\Delta}$, c'est-à-dire en effectuant la transposition $T = (x_2 x_3)$; soient

$$\psi_1 = x_1 + \omega x_2 + \omega^2 x_3 = \sqrt[3]{\frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right]},$$

$$\psi_1' = x_1 + \omega x_3 + \omega^2 x_2 = \sqrt[3]{\frac{1}{2}\left[S_1 + 3\sqrt{-3\Delta}\right]}$$

ces deux racines ; en y joignant la relation

$$-c_1 = x_1 + x_2 + x_3,$$

on a

$$3x_1 = -c_1 + \sqrt[3]{\frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right]} + \sqrt[3]{\frac{1}{2}\left[S_1 + 3\sqrt{-3\Delta}\right]},$$

$$3x_2 = -c_1 + \omega^2\sqrt{\frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right]} + \omega\sqrt[3]{\frac{1}{2}\left[S_1 + 3\sqrt{-3\Delta}\right]},$$

$$3x_3 = -c_1 + \omega\sqrt{\frac{1}{2}\left[S_1 - 3\sqrt{-3\Delta}\right]} + \omega^2\sqrt[3]{\frac{1}{2}\left[S_1 + 3\sqrt{-3\Delta}\right]}.$$

Il faut remarquer que ψ_1 et ψ_1' appartenant au même groupe, le groupe réduit à l'unité, s'expriment rationnellement l'un par l'autre ; en se servant des formules (4) pour exprimer $\psi_1' = x_1 + \omega x_3 + \omega^2 x_2$, on a précisément

$$\psi_1' = \frac{c_1^2 - 3c_2}{\psi_1};$$

on ne peut donc choisir arbitrairement que l'une des deux racines cubiques.

Les deux méthodes précédentes, qui sont identiques, reviennent à la détermination d'une racine de l'équation à laquelle satisfait la fonction ψ_1 ; c'est une équation du 6e degré que l'on obtient en

partant de l'équation (3), et qui est

$$(2\psi_1^3 - S_1)^2 + 27\Delta = 0.$$

Cette équation du sixième degré est l'équation résolvante de Lagrange, et elle se résout comme on l'a vu par deux équations binomes successives de degrés 2 et 3.

52. La méthode ordinairement employée pour arriver aux formules de Cardan revient à la précédente ; en effet, on commence par effectuer la transformation $x = -\frac{c_1}{3} + x'$, qui ramène l'équation à la forme $x'^3 + px' + q = 0$, puis on pose $x' = y + z$, et l'on détermine y et z par le système

$$yz = -\frac{p}{3}, \qquad y^3 + z^3 = -q,$$

qui est équivalent au suivant :

$$z = -\frac{p}{3y}, \qquad y^6 + qy^3 - \frac{p^3}{27} = 0;$$

on a ainsi à résoudre une équation du sixième degré pour déterminer y ; si y_1 est une racine, et z_1 la valeur correspondante de z, les six racines sont y_1, ωy_1, $\omega^2 y_1$, z_1, ωz_1, $\omega^2 z_1$, et les racines de l'équation donnée sont

$$x_1 = -\frac{c_1}{3} + y_1 + z_1,$$

$$x_2 = -\frac{c_1}{3} + \omega^2 y_1 + \omega z_1,$$

$$x_3 = -\frac{c_1}{3} + \omega y_1 + \omega^2 z_1;$$

on tire de là

$$3y_1 = x_1 + \omega x_2 + \omega^2 x_3,$$

$$3z_1 = x_1 + \omega^2 x_2 + \omega x_3,$$

de sorte que $3y_1$ et $3z_1$ ne sont autres que les fonctions ψ_1 et ψ'_1 qui nous ont servi dans la méthode de Lagrange, et les deux procédés sont identiques.

La discussion de l'équation du troisième degré est assez connue pour que nous ne la fassions pas ici.

53. Les équations spéciales irréductibles du troisième degré sont caractérisées par un groupe particulier ; le seul groupe transitif au-

tre que le groupe symétrique est le groupe alterné

$$[1, (x_1x_2x_3), (x_1x_3x_2)],$$

qui est en même temps le groupe des fonctions cycliques, puisqu'il est composé de la substitution circulaire $S = (x_1x_2x_3)$ et de ses puissances (§ 26) ; les seules équations spéciales du troisième degré sont donc celles pour lesquelles une fonction à deux valeurs fait partie du domaine de rationalité ; comme c'est aussi une fonction cyclique, l'équation devient, comme nous le verrons plus tard, une équation abélienne, et sa résolution exige seulement l'extraction d'une racine cubique et la connaissance des racines cubiques de l'unité. La condition nécessaire et suffisante pour qu'une équation du troisième degré jouisse de cette propriété est que le discriminant soit carré parfait ; en supposant l'équation mise sous la forme $x^3 + px + q = 0$, il est facile de former toutes les équations abéliennes à coefficients entiers ou fractionnaires ; si l'on pose

$$\Delta = -(4p^3 + 27q^2) = r^2, \qquad q = \lambda p, \qquad r = \mu p,$$

on a

$$p = -\frac{27\lambda^2 + \mu^2}{4}, \qquad q = -\lambda\frac{27\lambda^2 + \mu^2}{4}, \qquad r = -\mu\frac{27\lambda^2 + \mu^2}{4};$$

il suffit de donner à λ et μ toutes les valeurs rationnelles possibles pour avoir les équations répondant à la question.

54. L'équation générale du quatrième degré,

$$(1) \qquad f(x) = x^4 + c_1x^3 + c_2x^2 + c_3x + c_4 = 0,$$

a pour groupe symétrique G un groupe formé de 24 substitutions jouissant de propriétés particulières que nous avons déjà étudiées. Les principaux sous-groupes sont :

1° Le groupe alterné G′ d'ordre 12, dont nous avons déjà parlé au § 8 et formé des substitutions

$$\begin{array}{llll} 1, & (x_1x_2)(x_3x_4), & (x_1x_3)(x_2x_4), & (x_1x_4)(x_2x_3), \\ (x_1x_2x_3), & (x_1x_3x_2), & (x_1x_3x_4), & (x_1x_4x_3), \\ (x_1x_2x_4), & (x_1x_4x_2), & (x_2x_3x_4), & (x_2x_4x_3), \end{array}$$

2° Les groupes G_1, G_2, G_3 d'ordre 8, auxquels appartiennent les trois fonctions conjuguées

$$\varphi_1 = x_1x_2 + x_3x_4, \qquad \varphi_2 = x_1x_3 + x_2x_4, \qquad \varphi_3 = x_1x_4 + x_2x_3 \qquad (\S\ 15),$$

$$G_1 = [1,\ (x_1x_2),\ (x_3x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3),\ (x_1x_3x_2x_4),\ (x_1x_4x_2x_3)],$$

$$G_2 = [1,\ (x_1x_3),\ (x_2x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_4)(x_2x_3),\ (x_1x_2x_3x_4),\ (x_1x_4x_3x_2)],$$

$$G_3 = [1,\ (x_1x_4),\ (x_2x_3),\ (x_1x_4)(x_2x_3),\ (x_1x_3)(x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_3x_4x_2),\ (x_1x_2x_4x_3)];$$

ce sont des sous-groupes du groupe symétrique et non du groupe alterné.

3° Le groupe d'ordre 4,

$$H = [1,\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)],$$

auquel appartiennent la fonction

$$\omega_1 = x_1x_2 + x_3x_4 - x_1x_3 - x_2x_4 = (x_1 - x_4)(x_2 - x_3) = \varphi_1 - \varphi_2$$

(§ 21) et aussi la fonction

$$z_1 = \varphi_1 + \omega\varphi_2 + \omega^2\varphi_3 = (x_1x_2 + x_3x_4) + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3),$$

où ω est une racine cubique de l'unité (§ 25) ; le groupe H est un sous-groupe invariant du groupe symétrique et des groupes G', G_1, G_2, G_3, et c'est aussi le groupe commun avec trois groupes G_1, G_2, G_3.

4° Les groupes g_1, g_2, g_3 d'ordre 4 auxquels appartiennent respectivement les fonctions

$$\chi_1 = x_1 + x_2 - x_3 - x_4, \quad \chi_2 = x_1 + x_3 - x_2 - x_4, \quad \chi_3 = x_1 + x_4 - x_2 - x_3 \quad (\S\ 21),$$

$$g_1 = [1,\ (x_1x_2),\ (x_3x_4),\ (x_1x_2)(x_3x_4)],$$

$$g_2 = [1,\ (x_1x_3),\ (x_2x_4),\ (x_1x_3)(x_2x_4)],$$

$$g_3 = [1,\ (x_1x_4),\ (x_2x_3),\ (x_1x_4)(x_2x_3)];$$

g_1 est un sous-groupe invariant de G_1, de même g_2 de G_2 et g_3 de G_3.

5° Les groupes cycliques d'ordre 4 (§ 26),

$$C_1 = [1,\ (x_1x_3x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_4x_2x_3)],$$

$$C_2 = [1,\ (x_1x_2x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4x_3x_2)],$$

$$C_3 = [1,\ (x_1x_2x_4x_3),\ (x_1x_4)(x_2x_3),\ (x_1x_3x_4x_2)];$$

au premier appartient la fonction cyclique

$$w_1 = (x_1 + \omega x_3 + \omega^2 x_2 + \omega^3 x_4)^4,$$

où ω est une racine primitive de $\omega^4 - 1 = 0$, c'est-à-dire $+i$

ou $-i$; par suite à ces trois groupes appartiennent respectivement les fonctions cycliques

$$w_1 = [(x_1 - x_2) + i(x_3 - x_4)]^4, \qquad w'_1 = [(x_1 - x_2) - i(x_3 - x_4)]^4,$$
$$w_2 = [(x_1 - x_3) + i(x_2 - x_4)]^4, \qquad w'_2 = [(x_1 - x_3) - i(x_2 - x_4)]^4,$$
$$w_3 = [(x_1 - x_4) + i(x_2 - x_3)]^4, \qquad w'_3 = [(x_1 - x_4) - i(x_2 - x_3)]^4;$$

C_1, C_2 et C_3 sont des sous-groupes invariants des groupes G_1, G_2, G_3.

6° Les groupes d'ordre 2 (§ 8),

$$K_1 = [1, (x_1x_2)(x_3x_4)], \quad K_2 = [1, (x_1x_3)(x_2x_4)], \quad K_3 = [1, (x_1x_4)(x_2x_3)],$$

formés des carrés des substitutions circulaires précédentes, et auxquels appartiennent les fonctions

$$[(x_1-x_2)+i(x_3-x_4)]^2, \quad [(x_1-x_3)+i(x_2-x_4)]^2, \quad [(x_1-x_4)+i(x_2-x_3)]^2;$$

ce sont des sous-groupes invariants de H, ainsi que de C_1, C_2, C_3 et g_1, g_2, g_3.

Il existe d'autres groupes d'ordre 2,

$$\gamma_1 = [1, (x_1x_2)], \qquad \gamma'_1 = [1, (x_3x_4)], \qquad \gamma_2 = [1, (x_1x_3)], \qquad \ldots$$

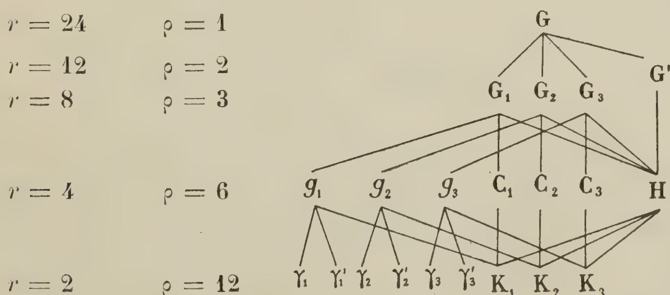
auxquels appartiennent des fonctions telles que

$$u_1(x_1 + x_2) + u_3x_3 + u_4x_4,$$

et qui sont respectivement des sous-groupes invariants de g_1, g_2 et g_3.

Nous ne considérerons pas les groupes d'ordre 6 auxquels appartiennent respectivement x_1, x_2, x_3 et x_4.

On peut résumer ce qui précède dans le tableau suivant .



55. On en déduit différentes méthodes de résolution :

1° Celle de Lagrange consiste, en partant des fonctions symétri-

ques, appartenant au groupe G, à calculer la valeur d'une fonction appartenant à l'un des trois groupes G_1, G_2, G_3, par exemple la fonction $\varphi_1 = x_1x_2 + x_3x_4$. Il faut pour cela calculer l'une des racines de l'équation du troisième degré à laquelle satisfont φ_1, φ_2, φ_3, et qui est (§ 15)

$$(2) \qquad \Phi(z) = z^3 + d_1z^2 + d_2z + d_3 = 0,$$

où

$$d_1 = -c_2, \qquad d_2 = c_1c_3 - 4c_4, \qquad d_3 = -c_3^2 + 4c_2c_4 - c_1^2c_4.$$

Lorsque l'on connaît φ_1, on peut calculer les fonctions appartenant au groupe g_1, qui est un sous-groupe invariant de G_1, par la résolution d'une équation du second degré ; en particulier les quatre fonctions $x_1 + x_2$, x_1x_2, $x_3 + x_4$ et x_3x_4 sont dans ce cas ; elles appartiennent au groupe g_1 et s'expriment rationnellement en fonction de l'une d'elles.

Si l'on considère par exemple la fonction $t_1 = x_1x_2$, elle a, pour les substitutions du groupe G_1, les deux valeurs t_1 et $t_2 = x_3x_4$ qui sont racines de l'équation

$$t^2 - \varphi_1 t + c_4 = 0;$$

lorsqu'on a déterminé une racine de cette équation, et qu'on la prend pour valeur de $t_1 = x_1x_2$, on peut exprimer les quatre fonctions dont nous venons de parler, car on a déjà, en désignant par t_2 l'autre racine,

$$x_1x_2 = t_1, \qquad x_3x_4 = t_2 = \varphi_1 - t_1,$$

puis

$$t_1(x_3 + x_4) + t_2(x_1 + x_2) = -c_3,$$

$$x_3 + x_4 + x_1 + x_2 = -c_1,$$

d'où

$$x_1 + x_2 = \frac{-c_3 + c_1t_1}{t_2 - t_1}, \qquad x_3 + x_4 = \frac{-c_3 + c_1t_2}{t_1 - t_2}.$$

Il ne reste plus qu'à résoudre deux équations du second degré ayant pour racines l'une x_1 et x_2, l'autre x_3 et x_4, connaissant respectivement la somme et le produit de ces quantités ; il suffit naturellement de calculer l'une des racines de chacune de ces équations, puisqu'on connaît déjà $x_1 + x_2$ et $x_3 + x_4$. On a ainsi les quatre racines de l'équation (1) en calculant une racine d'une équation du troisième degré (2) qui est la résolvante de Lagrange, et une racine de trois équations du second degré. On s'assure immédiatement

qu'un changement dans le choix de la racine que l'on calcule pour chacune des équations résolvantes successives revient à une permutation des indices des quatre racines x_1, x_2, x_3, x_4.

56. 2° Une modification apportée à la méthode de Lagrange consiste à prendre comme fonction du groupe g_1 au moyen de laquelle on veut calculer les autres

$$\chi_1 = x_1 + x_2 - x_3 - x_4\,;$$

pour les substitutions de G_1 elle a deux valeurs égales et de signes contraires, et l'on a (§ 21)

$$(3) \qquad \chi_1^2 = c_1^2 - 4c_2 + 4\varphi_1.$$

On peut donc calculer $x_1 + x_2$, x_1x_2, $x_3 + x_4$, x_3x_4 en fonction de χ_1, mais il est préférable d'opérer de la manière suivante :

La fonction χ_1 a six valeurs deux à deux égales et de signes contraires, et est racine d'une équation du sixième degré à coefficients symétriques ; on l'obtient soit directement, soit par l'élimination de φ_1 entre (2) et (3), ce qui donne, en posant $\chi_1^2 = \theta_1$,

$$(4) \quad \Phi(\theta) = \theta^3 + (8c_2 - 3c_1^2)\theta^2 + (3c_1^4 - 16c_1^2c_2 + 16c_1c_3 + 16c_2^2 - 64c_4)\theta - (c_1^3 - 4c_1c_2 + 8c_3)^2 = 0.$$

Soient $\theta_1, \theta_2, \theta_3$ les trois racines de cette équation ; les équations

$$\chi_1 = x_1 + x_2 - x_3 - x_4 = \sqrt{\theta_1},$$
$$\chi_2 = x_1 + x_3 - x_2 - x_4 = \sqrt{\theta_2},$$
$$\chi_3 = x_1 + x_4 - x_2 - x_3 = \sqrt{\theta_3},$$
$$x_1 + x_2 + x_3 + x_4 = -c_1$$

donnent

$$(5) \quad \begin{cases} x_1 = \dfrac{-c_1 + \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3}}{4}, \\[2ex] x_2 = \dfrac{-c_1 + \sqrt{\theta_1} - \sqrt{\theta_2} - \sqrt{\theta_3}}{4}, \\[2ex] x_3 = \dfrac{-c_1 - \sqrt{\theta_1} + \sqrt{\theta_2} - \sqrt{\theta_3}}{4}, \\[2ex] x_4 = \dfrac{-c_1 - \sqrt{\theta_1} - \sqrt{\theta_2} + \sqrt{\theta_3}}{4}; \end{cases}$$

mais il faut remarquer que, dès que l'on a choisi celle des deux va-

leurs de $\sqrt{\theta_1}$ que l'on prend pour χ_1 et celle des deux valeurs de $\sqrt{\theta_2}$ que l'on prend pour χ_2, χ_3 se trouve par cela même déterminé, et on ne peut choisir qu'une seule valeur de $\sqrt{\theta_3}$; la formule donnant x_1 ne présente ainsi que quatre déterminations qui sont les valeurs des quatre racines.

Cela tient à ce que le produit $\chi_1\chi_2\chi_3$ est symétrique, et que l'on a

$$(6)\quad \chi_1\chi_2\chi_3 = \Sigma x_1^3 - \Sigma x_1^2 x_2 + 2\Sigma x_1 x_2 x_3 = -(c_1^3 - 4c_1c_2 + 8c_3).$$

On a donc, au fond, à calculer deux racines d'une équation du troisième degré, et à prendre deux racines carrées. Remarquons que θ_1, θ_2, θ_3 appartiennent respectivement aux groupes G_1, G_2, G_3 et que la connaissance des trois racines de l'équation (4) entraîne celle des trois racines de l'équation (2), et réciproquement.

57. 3° La recherche d'une fonction cyclique, appartenant à l'un des groupes C_1, C_2, C_3, dépend d'une équation du sixième degré, mais comme ces groupes sont respectivement des sous-groupes invariants de G_1, G_2, G_3, on aura une fonction du groupe C_1 en extrayant la racine carrée d'une fonction du groupe G_1, et de même des autres ; ainsi les fonctions cycliques w_1, w'_1 sont telles que $w_1 + w'_1$ et $(w_1 - w'_1)^2$ appartiennent au groupe G_1 et s'expriment rationnellement en fonction de φ_1.

On a en effet

$$\begin{aligned} w_1 + w'_1 &= 2[(x_1 - x_2)^4 - 6(x_1 - x_2)^2(x_3 - x_4)^2 + (x_3 - x_4)^2] \\ &= 4[(x_1 - x_2)^2 - (x_3 - x_4)^2]^2 - 2[(x_1 - x_2)^2 + (x_3 - x_4)^2]^2 \\ &= 4\theta_2\theta_3 - 2(c_1^2 - 2c_2 - 2\varphi_1)^2 \end{aligned}$$

et, d'après les équations (3) et (4), $\theta_2\theta_3$ s'exprime rationnellement au moyen de θ_1 ou de φ_1 par la formule

$$\theta_1\theta_2\theta_3 = (c_1^2 - 4c_2 + 4\varphi_1)\theta_2\theta_3 = (c_1^3 - 4c_1c_2 + 8c_3)^2 ;$$

de plus

$$[(x_1 - x_2) + i(x_3 - x_4)][(x_1 - x_2) - i(x_3 - x_4)] = c_1^2 - 2c_2 - 2\varphi_1,$$

de sorte que l'on a

$$w_1 w'_1 = (c_1^2 - 2c_2 - 2\varphi_1)^4$$

et w_1, ainsi que w'_1, sont racines de l'équation

$$(7)\quad w^2 - [4\theta_2\theta_3 - 2(c_1^2 - 2c_2 - 2\varphi_1)^2]w + (c_1^2 - 2c_2 - 2\varphi_1)^4 = 0.$$

Ayant ainsi w_1 par exemple, la fonction

$$(x_1 - x_2) + i(x_3 - x_4) = \sqrt[4]{w_1}$$

est une fonction de Galois au moyen de laquelle s'expriment les autres, ainsi que les racines elles-mêmes ; le calcul de x_1, x_2, x_3, x_4 en fonction de $\sqrt[4]{w_1}$ est compliqué ; on peut le remplacer par le suivant, dont nous retrouverons la généralisation dans la théorie des équations abéliennes :

Dans la fonction $\sqrt[4]{w_1} = x_1 + ix_3 + i^2x_2 + i^3x_4$ remplaçons i par i^2 et i^3 ; nous obtenons les nouvelles fonctions

$$\chi_1 = x_1 - x_3 + x_2 - x_4, \qquad \sqrt[4]{w'_1} = x_1 - ix_3 + x_2 + ix_4 ;$$

les produits

$$(x_1 - x_3 + x_2 - x_4)(x_1 + ix_3 - x_2 - ix_4)^{-2} = \text{A},$$

$$(x_1 - ix_3 - x_2 + ix_4)(x_1 + ix_3 - x_2 - ix_4)^{-3} = \text{B}$$

restent invariables pour le groupe C_1 et s'expriment rationnellement au moyen de w_1 ; leurs valeurs sont

$$\text{A} = \frac{\chi_1}{w_1}\left[\chi_2\chi_3 + \frac{1}{4}\,\frac{w_1 - w'_1}{\chi_2\chi_3}\right] = \frac{\theta_1[w_1 + (c_1^2 - 2c_2 - 2\varphi_1)^2]}{2w_1\chi_1\chi_2\chi_3},$$

$$\text{B} = \frac{\sqrt[4]{w_1}\sqrt[4]{w'_1}}{w_1} = \frac{c_1^2 - 2c_2 - 2\varphi_1}{w_1}.$$

Elles sont bien rationnelles par rapport à w_1, car l'équation (6) donne la valeur de $\chi_1\chi_2\chi_3$, et nous avons reconnu précédemment que l'on a

$$\text{(8)} \qquad \sqrt[4]{w_1}\sqrt[4]{w'_1} = c_1^2 - 2c_2 - 2\varphi_1 ;$$

dès lors les équations

$$x_1 + ix_3 - x_2 - ix_4 = \sqrt[4]{w_1},$$

$$x_1 - x_3 + x_2 - x_4 = \text{A}(\sqrt[4]{w_1})^2,$$

$$x_1 - ix_3 - x_2 + ix_4 = \text{B}(\sqrt[4]{w_1})^3,$$

$$x_1 + x_2 + x_3 + x_4 = -c_1$$

donnent

$$\text{(9)} \qquad x_1 = \frac{-c_1 + \sqrt[4]{w_1} + \text{A}(\sqrt[4]{w_1})^2 + \text{B}(\sqrt[4]{w_1})^3}{4}$$

et des expressions analogues pour les autres racines ; elles sont de même forme que celles qu'a données Euler.

On a de cette façon à calculer une racine d'une équation du troisième degré, puis une racine d'une équation du second degré, et à extraire une racine quatrième.

58. 4° En partant des fonctions symétriques appartenant au groupe G, on peut calculer une fonction appartenant au groupe alterné G' par l'extraction d'une racine carrée, puis une fonction appartenant au groupe H par l'extraction d'une racine cubique. Comme nous l'avons vu au § 25, la fonction

$$z_1 = \varphi_1 + \omega\varphi_2 + \omega^2\varphi_3 = (x_1x_2 + x_3x_4) + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3),$$

où ω est une racine cubique imaginaire de l'unité, est racine d'une équation binome de degré 3 dont les coefficients appartiennent au groupe alterné. Cette fonction z_1 n'est autre que la fonction de Galois relative à la résolution de l'équation du troisième degré (2) ayant pour racines φ_1, φ_2, φ_3, lorsqu'on emploie la méthode de Lagrange ; on a, en adjoignant les racines cubiques de l'unité ou $\sqrt{-3}$,

$$(10) \qquad z_1^3 = \frac{1}{2}\left[-2d_1^3 + 9d_1d_2 - 27d_3 - 3\sqrt{-3}\sqrt{\Delta}\right],$$

où d_1, d_2, d_3 sont les coefficients, et Δ le discriminant de l'équation (2); Δ est identique au discriminant de l'équation du 4e degré, comme nous l'avons déjà vu au § 15.

Ce discriminant,

$$\Delta = -4d_2^3 - 27d_3^2 + 18d_1d_2d_3 + d_1^2d_2^2 - 4d_1^3d_3,$$

peut être mis sous la forme particulière $-(4P^3 + 27Q^2)$ si l'on applique à l'équation (2) la transformation

$$z = -\frac{d_1}{3} + z'$$

qui fait disparaître le deuxième terme ; on a alors

$$\Delta = -4\left(d_2 - \frac{d_1^2}{3}\right)^3 - 27\left(d_3 - \frac{d_1d_2}{3} + \frac{2d_1^3}{27}\right)^2,$$

ou, en remplaçant d_1, d_2, d_3 par leurs valeurs,

$$\Delta = -4\left(c_1c_3 - 4c_4 - \frac{c_2^2}{3}\right)^2 - 27\left(-c_3^2 + 4c_2c_4 - c_1^2c_4 + \frac{c_1c_2c_3}{3} - \frac{4c_2c_4}{3} - \frac{2c_2^3}{27}\right)^2.$$

Les fonctions symétriques

$$P = c_1c_3 - 4c_4 - \frac{c_2^2}{3},$$

$$Q = -c_3^2 + 4c_2c_4 - c_1^2c_4 + \frac{c_1c_2c_3}{3} - \frac{4c_2c_4}{3} - \frac{2c_2^3}{27}$$

jouent un rôle particulier dans la théorie des invariants des formes binaires ; si l'on écrit l'équation (1) sous la forme

$$f(x) = ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0,$$

on a (*)

$$\Delta = \frac{4^4}{a^6}(S^3 - 27T^2),$$

où

$$S = ae - 4bd + 3c^2, \qquad T = \begin{vmatrix} a & b & c \\ b & c & d \\ c & d & e \end{vmatrix}.$$

La recherche de la fonction précédente z_1 appartenant au groupe H est équivalente à la détermination des trois fonctions $\varphi_1, \varphi_2, \varphi_3$, et aussi à celle des trois fonctions $\theta_1, \theta_2, \theta_3$ employées dans la deuxième méthode ; on peut donc, après avoir calculé z_1, déterminer $\varphi_1, \varphi_2, \varphi_3$ comme nous avons déterminé les racines x_1, x_2, x_3 de l'équation du troisième degré au moyen de ψ_1 par les formules (4) du § 51, puis en déduire $\theta_1, \theta_2, \theta_3$, et enfin x_1, x_2, x_3, x_4 par les formules (5) du § 56.

La méthode que nous venons d'indiquer n'est donc pas nouvelle ; elle consiste simplement dans l'application de la méthode de Lagrange à la résolution de l'équation du troisième degré (2) (§ 55) ; mais, en suivant le tableau des groupes de quatre variables, on voit qu'on peut, en partant de z_1, déterminer une fonction de l'un des groupes K_1, K_2, K_3 par l'extraction d'une racine carrée ; en prenant

$$v_1 = [(x_1 - x_2) + i(x_3 - x_4)]^2, \qquad v_1' = [(x_3 - x_4) + i(x_1 - x_2)]^2$$

on a les deux valeurs conjuguées, pour les substitutions du groupe H, d'une fonction appartenant au groupe K_1 ; leurs fonctions symétriques sont déterminées par les formules

$$(11) \quad v_1 + v_1' = 4i(x_1 - x_2)(x_3 - x_4) = 4i(\varphi_2 - \varphi_3) = \frac{4i(\omega - 1)}{3\omega^2}\,\frac{z_1^2 - d_1^2 + 3d_2}{z_1},$$

$$(12) \quad \sqrt{v_1}\sqrt{v_1'} = i[(x_1 - x_2)^2 + (x_3 - x_4)^2] = i(c_1^2 - 2c_2 - 2\varphi_1)$$

$$= i\left[c_1^2 - 2c_2 - 2\frac{z_1^2 - d_1z_1 + d_1^2 - 3d_2}{3z_1}\right].$$

On a ainsi l'équation du second degré dont v_1 et v_1' sont les racines.

(*) Salmon, *Leçons d'Algèbre supérieure*, p. 270.

Connaissant v_1, une extraction de racine carrée donne la fonction de Galois $x_1 + ix_3 - x_2 - ix_4$ au moyen de laquelle on peut calculer les racines, ou bien encore, on peut poser

$$(x_1 - x_2) + i(x_3 - x_4) = \sqrt{v_1},$$
$$i(x_1 - x_2) + (x_3 - x_4) = \sqrt{v_1'},$$

où les signes sont déterminés en fonction l'un de l'autre par la relation (12) ; de plus $x_1 + x_2 - x_3 - x_4 = \chi_1$ est une fonction du groupe g_1 dont K_1 est un sous-groupe, et s'exprime rationnellement au moyen de v_1 ; on aura sa valeur en se reportant à la manière dont $A = \chi_1 v_1^{-1}$ a été déterminé dans le § précédent ; θ_1 et φ_1 s'expriment au moyen de z_1, et w_1 est égal à v_1^2, de sorte que l'on obtient la valeur de χ_1 en fonction de v_1 et de z_1. En joignant aux formules précédentes la relation $x_1 + x_2 + x_3 + x_4 = -c_1$, on a

$$(13)\qquad \begin{cases} 4x_1 = -c_1 + \chi_1 + \sqrt{v_1} - i\sqrt{v_1'}, \\ 4x_2 = -c_1 + \chi_1 - \sqrt{v_1} + i\sqrt{v_1'}, \\ 4x_3 = -c_1 - \chi_1 - i\sqrt{v_1} + \sqrt{v_1'}, \\ 4x_4 = -c_1 - \chi_1 + i\sqrt{v_1} - \sqrt{v_1'}. \end{cases}$$

Nous mentionnerons encore la manière d'arriver à la fonction de Galois $x_1 - x_2 + ix_3 - ix_4$ par la suite des groupes G, G_1, g_1, K_1 ; la fonction v_1 est déterminée au moyen de χ_1 appartenant au groupe g_1 par l'extraction d'une racine carrée ; en posant

$$v_1 = (x_1 - x_2 + ix_3 - ix_4)^2, \qquad v_1'' = (x_1 - x_2 - ix_3 + ix_4)^2,$$

on a

$$(14)\quad v_1 + v_1'' = 2(x_1 - x_2)^2 - 2(x_3 - x_4)^2 = 2\chi_2\chi_3 = \frac{-2(c_1^3 - 4c_1c_2 + 8c_3)}{\chi_1},$$

$$(15)\quad \sqrt{v_1}\sqrt{v_1''} = (x_1 - x_2)^2 + (x_3 - x_4)^2 = c_1^2 - 2c_2 - 2\varphi_1 = \frac{1}{2}(3c_1^2 - 8c_2 - \chi_1^2),$$

d'après les formules (6) et (3) ; on a ainsi v_1 en fonction de χ_1 ; on en déduit les racines x par la formule

$$(16)\qquad 4x_1 = -c_1 + \chi_1 + \sqrt{v_1} + \sqrt{v_1''},$$

et d'autres analogues qui se déduisent de (13) en remplaçant $\sqrt{v_1'}$ par $i\sqrt{v_1'}$.

Enfin, on peut calculer la fonction de Galois par la suite des groupes G, G_1, g_1, γ_1, en résolvant deux équations du second degré après avoir déterminé χ_1.

59. La méthode de Ferrari consiste à décomposer le premier membre de l'équation du quatrième degré en un produit de deux facteurs du second degré ; je vais montrer qu'elle revient à la méthode de Lagrange.

Supposons que l'on ait effectué une décomposition de $f(x)$ sous la forme

$$(1)\quad f(x) = x^4 + c_1x^3 + c_2x^2 + c_3x + c_4 = (x^2 + \alpha x + \beta)(x^2 + \alpha' x + \beta').$$

On peut remplacer le produit des deux trinomes par une différence de deux carrés,

$$\left(x^2 + \frac{\alpha + \alpha'}{2}x + \frac{\beta + \beta'}{2}\right)^2 - \left(\frac{\alpha - \alpha'}{2}x + \frac{\beta - \beta'}{2}\right)^2;$$

comme $\alpha + \alpha' = c_1$, le premier terme peut s'écrire, en posant $\beta + \beta' = \lambda$, $\left(x^2 + \frac{c_1}{2}x + \frac{\lambda}{2}\right)^2$, et le polynome $f(x)$ est égal à

$$f(x) = \left(x^2 + \frac{c_1}{2}x + \frac{\lambda}{2}\right)^2 - \left(\frac{\alpha - \alpha'}{2}x + \frac{\beta - \beta'}{2}\right)^2.$$

Comme on a d'autre part identiquement

$$(2)\quad f(x) = \left(x^2 + \frac{c_1}{2}x + \frac{\lambda}{2}\right)^2 - \left[\left(\lambda + \frac{c_1^2}{4} - c_2\right)x^2 + \left(\frac{\lambda c_1}{2} - c_3\right)x + \left(\frac{\lambda^2}{4} - c_4\right)\right],$$

il faut que λ satisfasse à la condition que le dernier trinome soit carré parfait, et cette condition, qui est nécessaire, est aussi suffisante, de sorte qu'à chaque décomposition de $f(x)$ sous la forme (1) correspond une décomposition analogue sous la forme (2), où le second trinome est carré parfait, et réciproquement.

Or, *a priori*, on peut mettre le polynome $f(x)$ de trois manières et trois seulement sous la forme (1), en désignant par x_1, x_2, x_3, x_4 les racines de l'équation ; ce sont

$$f(x) = [x^2 - (x_1 + x_2)x + x_1x_2][x^2 - (x_3 + x_4)x + x_3x_4],$$
$$f(x) = [x^2 - (x_1 + x_3)x + x_1x_3][x^2 - (x_2 + x_4)x + x_2x_4],$$
$$f(x) = [x^2 - (x_1 + x_4)x + x_1x_4][x^2 - (x_2 + x_3)x + x_2x_3];$$

il existe donc trois valeurs de λ satisfaisant aux conditions imposées, correspondantes à ces trois manières; comme $\lambda = \beta + \beta'$, et que β et β' sont les termes constants des deux trinomes dans les-

quels $f(x)$ est décomposé, on voit que les trois valeurs de λ sont égales à

$$\lambda_1 = x_1x_2 + x_3x_4, \qquad \lambda_2 = x_1x_3 + x_2x_4, \qquad \lambda_3 = x_1x_4 + x_2x_3\,;$$

ce sont les trois racines $\varphi_1, \varphi_2, \varphi_3$ de l'équation résolvante de Lagrange ; on le vérifie du reste en formant l'équation à laquelle satisfait λ :

$$(3) \qquad \Phi(\lambda) = 4\left(\lambda + \frac{c_1^2}{4} - c_2\right)\left(\frac{\lambda^2}{4} - c_4\right) - \left(\lambda\frac{c_1}{2} - c_3\right)^2 = 0\,;$$

elle est identique à l'équation (2) (§ 55) ayant pour racines $\varphi_1, \varphi_2, \varphi_3$.

Lorsqu'on a déterminé une racine λ_1 de cette équation, et qu'on lui attribue la valeur $x_1x_2 + x_3x_4$, la décomposition effective en un produit de deux trinomes de $f(x)$ qui, sous la forme (2), est une différence de deux carrés, donne précisément

$$f(x) = [x^2 - (x_1 + x_2)x + x_1x_2][x^2 - (x_3 + x_4)x + x_3x_4]\,;$$

il en résulte que les coefficients des deux trinomes obtenus, qui contiennent la racine carrée d'une fonction entière de λ_1, sont les valeurs des quatre quantités $x_1 + x_2$, x_1x_2, $x_3 + x_4$, x_3x_4. On est donc amené, par la méthode actuelle, à déterminer en fonction de λ_1 les quatre fonctions précédentes des racines, puis à résoudre deux équations du second degré ; c'est ce que l'on fait précisément dans la méthode de Lagrange.

On peut ajouter que $\lambda + \dfrac{c_1^2}{4} - c_2$ est égal à $\left(\dfrac{\alpha - \alpha'}{2}\right)^2$; comme α et α' sont égaux respectivement aux sommes de deux racines, les trois valeurs que prend cette quantité sont

$$\frac{1}{4}(x_1 + x_2 - x_3 - x_4)^2, \quad \frac{1}{4}(x_1 + x_3 - x_2 - x_4)^2, \quad \frac{1}{4}(x_1 + x_4 - x_2 - x_3)^2,$$

c'est-à-dire $\dfrac{1}{4}\theta_1$, $\dfrac{1}{4}\theta_2$, $\dfrac{1}{4}\theta_3$. Nous vérifions de cette façon que λ ou φ et θ sont liés l'un à l'autre par la relation

$$\theta = c_1^2 - 4c_2 + 4\varphi.$$

60. Nous allons appliquer l'étude de la nature des racines de l'équation résolvante $\Phi(\lambda) = 0$ à la discussion de l'équation du quatrième degré ; nous nous placerons dans le cas où les coefficients de celle-ci sont réels, et nous chercherons la réalité et l'ordre de multiplicité des racines x_1, x_2, x_3, x_4.

D'après la remarque déjà faite que le discriminant de $\Phi(\lambda)$ est le même que celui de $f(x)$, la condition nécessaire et suffisante pour que les racines x soient distinctes est qu'il en soit de même de $\lambda_1, \lambda_2, \lambda_3$.

En étudiant les différents cas qui peuvent se présenter pour les racines x, on arrive à des conclusions différentes relativement aux racines λ et au signe de $\lambda + \frac{c_1^2}{4} - c_2$, de sorte que les réciproques sont exactes, et qu'on peut énoncer les résultats suivants :

I. $\lambda_1, \lambda_2, \lambda_3$ distincts : les racines x_1, x_2, x_3, x_4 le sont également.

1° $\lambda_1, \lambda_2, \lambda_3$ réels et $\geqslant c_2 - \frac{c_1^2}{4}$: les quatre racines x sont réelles.

2° $\lambda_1, \lambda_2, \lambda_3$ réels ; un au moins $< c_2 - \frac{c_1^2}{4}$: les quatre racines sont imaginaires.

3° λ_1 réel, λ_2, λ_3 imaginaires : deux racines sont réelles et deux imaginaires.

II. $\lambda_2 = \lambda_3 \neq \lambda_1$: l'équation a au moins une racine double $x_1 = x_2$.

1° $\lambda_2 > c_2 - \frac{c_1^2}{4}$: trois racines réelles et distinctes, dont une double.

2° $\lambda_2 < c_2 - \frac{c_1^2}{4}$: une racine double réelle et deux imaginaires.

3° $\lambda_2 = c_2 - \frac{c_1^2}{4}$, $\lambda_1 > c_2 - \frac{c_1^2}{4}$: deux racines doubles réelles $x_1 = x_2$, $x_3 = x_4$.

4° $\lambda_2 = c_2 - \frac{c_1^2}{4}$, $\lambda_1 < c_2 - \frac{c_1^2}{4}$: deux racines doubles imaginaires.

III. $\lambda_1 = \lambda_2 = \lambda_3$: l'équation a au moins une racine triple.

1° $\lambda_1 \neq c_2 - \frac{c_1^2}{4}$: une racine triple et une simple.

2° $\lambda_1 = c_2 - \frac{c_1^2}{4}$: une racine quadruple.

Il serait facile d'exprimer les conditions précédentes au moyen des coefficients de $f(x)$; j'indiquerai simplement que la condition nécessaire et suffisante pour que l'équation ait une racine double est exprimée par l'égalité $\Delta = -(4P^3 + 27Q^2) = 0$, où P et Q

ont les valeurs données au § 58, et que les conditions nécessaires et suffisantes pour qu'elle ait une racine triple sont exprimées par $P = 0$ et $Q = 0$ ou bien par $S = 0$, $T = 0$.

On obtiendrait des résultats analogues en discutant l'équation résolvante ayant pour racines θ_1, θ_2, θ_3 ; on peut ajouter que parmi les trois décompositions de $f(x)$ en trinomes du second degré, il en existe toujours au moins une à coefficients réels.

61. Les équations spéciales du quatrième degré irréductibles sont caractérisées par un groupe particulier satisfaisant à la condition d'être transitif ; les groupes transitifs à quatre variables sont les suivants, après le groupe symétrique : 1° le groupe alterné G' ; 2° l'un des groupes d'ordre 8 : G_1, G_2, G_3 ; 3° le sous-groupe invariant H ; 4° l'un des groupes cycliques : C_1, C_2, C_3.

Les équations ayant pour groupe G' sont caractérisées par ce fait que le discriminant est carré parfait dans le domaine de rationalité ; alors les fonctions φ_1, φ_2, φ_3 et z_1 s'obtiennent par l'extraction d'une racine cubique après adjonction de la racine de l'unité ω.

Celles qui ont pour groupe G_1, G_2 ou G_3 sont telles que l'équation résolvante de Lagrange, ou bien l'équation $\Phi(\theta) = 0$ aient une racine rationnelle ; les méthodes que nous avons données s'appliquent à leur résolution et les racines s'obtiennent par l'extraction de trois racines carrées ; les équations bicarrées et les équations réciproques appartiennent à cette classe.

Celles qui ont pour groupe H sont telles que les trois racines de l'équation résolvante de Lagrange s'expriment rationnellement dans le domaine ; les formules (11), (12) et (13) indiquent comment on les résout par deux extractions de racine carrée. Enfin celles qui ont pour groupe l'un des groupes cycliques C_1, C_2, C_3 sont des équations abéliennes ; les formules (9) montrent que leurs racines s'expriment au moyen d'une seule racine quatrième portant sur une quantité connue.

62. Nous venons de voir que l'on peut résoudre les équations du deuxième, du troisième et du quatrième degré en cherchant une fonction de Galois de la forme

$$\psi_1 = x_1 + \omega x_2 + \omega^2 x_3 + \dots + \omega^{n-1} x_n,$$

où ω est une racine primitive de $x^n - 1 = 0$ que l'on adjoint,

dans le courant du calcul, au domaine de rationalité. Lagrange, dans son mémoire dont nous avons déjà parlé, a cherché à généraliser cette méthode pour une équation de degré quelconque supposée générale ; il n'est pas parvenu à résoudre les équations de degré supérieur à quatre, et nous verrons que c'est impossible, mais ses recherches sont importantes pour la résolution de certaines équations spéciales, et nous allons les résumer.

Supposons d'abord que le degré n de l'équation soit premier ; d'après ce que nous avons vu au chapitre V, la fonction

$$w_1 = \psi_1^n = (x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{n-1} x_n)^n$$

est une fonction cyclique admettant $(n-1)!$ valeurs pour toutes les substitutions ; mais, parmi ces valeurs, il en existe $n-1$ particulières appartenant au même groupe que w_1 ; ce sont les fonctions $w_1, w_2, \ldots, w_{n-1}$ obtenues en remplaçant dans la précédente ω par chacune des racines de l'équation binome $x^n - 1 = 0$ autres que l'unité, racines que nous avons désignées par

$$\omega^g, \omega^{g^2}, \ldots, \omega^{g^{n-1}};$$

ces fonctions $w_1, w_2, \ldots, w_{n-1}$, qui s'expriment rationnellement au moyen de l'une d'entre elles, sont elles-mêmes telles que la fonction cyclique

$$\mu = \gamma^{n-1} = (w_1 + \alpha w_2 + \alpha^2 w_3 + \cdots + \alpha^{n-2} w_{n-1})^{n-1},$$

où α est racine primitive de $x^{n-1} - 1 = 0$, appartienne au groupe métacyclique que nous avons désigné par

$$M = | z \quad az + b | \quad (\text{mod. } n) \quad \begin{pmatrix} a = 1, 2, \ldots, n-1 \\ b = 0, 1, 2, \ldots, n-1 \end{pmatrix}.$$

La fonction μ est racine d'une équation de degré $(n-2)!$ à coefficients symétriques ; si l'on connaît une racine de cette équation, on peut calculer $x_1, x_2, \ldots, x_n$ par de simples extractions de racines, après adjonction des racines de l'unité ω et α, comme nous allons le montrer.

On peut d'abord supposer les indices des racines x choisis de façon que la quantité connue soit la fonction μ précédente ; en prenant une racine d'indice $n-1$, on a la fonction

$$\gamma = w_1 + \alpha w_2 + \cdots + \alpha^{n-2} w_{n-1} = \sqrt[n-1]{\mu};$$

elle appartient au groupe de w_1 ; c'est de plus, par rapport aux élé-

ments $w_1, w_2, \ldots, w_{n-1}$, une fonction de Galois, et l'on peut calculer ces éléments d'une manière rationnelle au moyen de γ et des fonctions symétriques des $n-1$ quantités w. Ces dernières fonctions symétriques, restant invariables par les substitutions du groupe M, s'expriment rationnellement en fonction de μ et des coefficients de l'équation donnée ; par suite $w_1, w_2, \ldots, w_{n-1}$ peuvent être calculés rationnellement au moyen de μ et de γ.

Ayant ainsi w_1, une extraction de racine n^e donne la fonction de Galois

$$\psi_1 = x_1 + \omega x_2 + \cdots + \omega^{n-1} x_n = \sqrt[n]{w_1},$$

au moyen de laquelle s'expriment les racines x elles-mêmes ; il est plus simple de prendre à la fois les $n-1$ fonctions cycliques $w_1, w_2, \ldots, w_{n-1}$; en désignant par $\omega_1, \omega_2, \ldots, \omega_{n-1}$ les racines de l'unité qui y entrent respectivement, on a

$$\begin{aligned}
x_1 + \omega_1 x_2 + \cdots + \omega_1^{n-1} x_n &= \sqrt[n]{w_1},\\
x_1 + \omega_2 x_2 + \cdots + \omega_2^{n-1} x_n &= \sqrt[n]{w_2},\\
\cdots\cdots\cdots\cdots &\cdots,\\
x_1 + \omega_{n-1} x_2 + \cdots + \omega_{n-1}^{n-1} x_n &= \sqrt[n]{w_{n-1}},\\
x_1 + x_2 + \cdots + x_n &= -c_1,
\end{aligned}$$

d'où l'on tire

$$\begin{aligned}
nx_1 &= -c_1 + \sqrt[n]{w_1} + \sqrt[n]{w_2} + \cdots \sqrt[n]{w_{n-1}},\\
nx_2 &= -c_1 + \omega_1^{-1}\sqrt[n]{w_1} + \omega_2^{-1}\sqrt[n]{w_2} + \cdots + \omega_{n-1}^{-1}\sqrt[n]{w_{n-1}},\\
\cdots\cdots &\cdots\cdots\cdots\cdots
\end{aligned}$$

Ainsi donc, on résout l'équation de degré n, n étant premier : 1° en calculant une racine d'une équation de degré $(n-2)!$; 2° en extrayant une racine d'indice $n-1$ et une autre d'indice n.

L'équation résolvante de degré $(n-2)!$ ayant pour racines les fonctions métacycliques conjuguées est, pour $n \geqslant 5$, d'un degré supérieur à n, et la difficulté du problème n'est que reculée ; cependant si une équation spéciale est telle qu'une fonction métacyclique soit connue et fasse partie du domaine de rationalité, cette équation est résoluble par radicaux ; nous démontrerons plus loin la réciproque de cette proposition fondamentale.

63. Considérons maintenant le cas où le degré de l'équation est un nombre composé ; soit $n = pq$, où p est un nombre premier ; nous allons ramener la résolution de l'équation donnée à

celle de p équations de degré q ; partageons pour cela les n racines $x_1, x_2, \ldots, x_n$ en p séries, et formons les sommes

$$X_1 = x_1 + x_{p+1} + x_{2p+1} \cdots + x_{(q-1)p+1},$$
$$X_2 = x_2 + x_{p+2} + \cdots + x_{(q-1)p+2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$X_p = x_p + x_{2p} + \cdots + x_{qp}$$

des racines de chacune d'elles; si elles sont connues, on peut calculer toutes les fonctions symétriques des racines de chaque série, car elles appartiennent au même groupe de substitutions que la somme X correspondante, et s'expriment rationnellement au moyen de cette somme et des coefficients de l'équation.

La connaissance des fonctions $X_1, X_2, \ldots, X_p$ entraîne ainsi celle des coefficients des p équations dans lesquelles se décompose l'équation donnée.

Pour déterminer les quantités X, nous formerons l'équation de degré p dont elles sont les racines,

$$F(X) = X^p + C_1X^{p-1} + C_2X^{p-2} + \cdots + C_p = 0.$$

Les coefficients appartiennent tous à un même groupe de substitutions des variables x, celui que l'on obtient en permutant dans chaque série les éléments x de toutes les manières possibles, et en permutant les séries entre elles ; il a pour ordre $(q\,!)^p p\,!$, de sorte que $C_1, C_2, \ldots, C_p$ s'expriment rationnellement au moyen d'une seule fonction y appartenant au groupe précédent, et racine d'une équation de degré $\frac{n\,!}{p\,!(q\,!)^p}$.

Quant aux racines de l'équation $F(X) = 0$, on les obtiendra, puisque p est premier, en appliquant la méthode précédemment décrite, c'est-à-dire en résolvant une équation de degré $(p-2)\,!$ et extrayant des racines d'indices $p-1$ et p.

On a donc, en posant $n = pq$, où p est premier : 1° à calculer une racine y d'une équation de degré $\frac{n\,!}{p\,!(q\,!)^p}$ à coefficients connus; 2° à calculer une racine d'une équation de degré $(p-2)\,!$ dont les coefficients sont des fonctions rationnelles de la racine y calculée ; 3° à extraire une racine d'indice $p-1$ et une autre d'indice p ; 4° à résoudre p équations de degré q. Si q est un nombre

composé, on pourra répéter ce qui précède pour ces nouvelles équations.

Ainsi, par exemple, pour $n = 4$, $p = q = 2$, la méthode précédente conduit à poser $X_1 = x_1 + x_3$, $X_2 = x_2 + x_4$; les coefficients de l'équation $F(X) = 0$ dépendent d'une racine d'une équation du troisième degré qui est précisément l'équation résolvante de Lagrange ; on a alors X_1 et X_2 en extrayant la racine carrée d'une fonction rationnelle par rapport à φ_1, et il reste à résoudre deux équations du second degré.

Pour $n > 4$, l'équation résolvante de degré $\frac{n!}{p!(q!)^p}$ est d'un degré supérieur à n ; il n'y a que pour des équations spéciales que les recherches précédentes conduisent à la résolution d'une équation de degré > 4.

CHAPITRE IX

DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS (*)

64. Soit une équation de degré n,

$$(1) \quad f(x, R', R'', \dots) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n = 0;$$

nous supposons que les coefficients font partie du domaine de rationalité $(R', R'', \dots)$, défini par des paramètres arbitraires et indépendants $R', R'', \dots$ comme nous l'avons expliqué au chapitre VI, et que le polynome $f(x)$ est irréductible dans ce domaine ; nous dirons que l'équation est résoluble algébriquement si l'on peut y satisfaire identiquement en substituant à x une expression formée au moyen des éléments du domaine et des signes des opérations suivantes de l'algèbre : addition, soustraction, multiplication, division, élévation à une puissance d'exposant entier, extraction de racine d'indice entier, en nombre limité ; nous dirons aussi que l'équation est résoluble par radicaux.

Comme l'extraction d'une racine d'indice pq se ramène à deux extractions successives de racines d'indices p et q, on peut toujours supposer que les radicaux qui entrent dans l'expression de la racine sont d'indice premier ; c'est ce que nous ferons désormais.

Avant de chercher si une équation est résoluble algébriquement, il est nécessaire d'étudier la formation des expressions algébriques. La suite des calculs à effectuer pour arriver à une telle expression peut toujours se ramener à la série suivante d'opérations :

(*) Ce chapitre est extrait, en grande partie, de l'ouvrage déjà cité de M. Netto, *Substitutionentheorie*, chap. 13, p. 235.

1° Calcul d'une fonction rationnelle des éléments du domaine

$$F_\nu(R', R'', \ldots).$$

2° Calcul d'une racine V_ν d'indice premier p_ν de cette fonction rationnelle ; nous supposons que F_ν n'est pas la puissance exacte d'ordre p_ν d'une fonction du domaine donné, car sinon on prendrait cette fonction comme valeur de V_ν, qui ferait ainsi partie du domaine primitif ; V_ν est par suite une quantité nouvelle définie par l'équation

$$V_\nu^{p_\nu} = F_\nu(R', R'', \ldots).$$

3° Adjonction de V_ν au domaine, formation d'une fonction rationnelle $F_{\nu-1}(V_\nu, R', R'', \ldots)$ du domaine ainsi étendu, et extraction d'une racine $V_{\nu-1}$ d'indice premier $p_{\nu-1}$ de cette fonction ; $F_{\nu-1}$ peut ne pas contenir V_ν, mais n'est pas une puissance exacte d'ordre $p_{\nu-1}$ d'une fonction du nouveau domaine $(V_\nu, R', R'', \ldots)$, car sinon $V_{\nu-1}$ en ferait partie ; c'est donc une nouvelle quantité définie par

$$V_{\nu-1}^{p_{\nu-1}} = F_{\nu-1}(V_\nu, R', R'', \ldots).$$

4° Adjonction de $V_{\nu-1}$ au domaine déjà formé, formation d'une fonction rationnelle du nouveau domaine $F_{\nu-2}(V_{\nu-1}, V_\nu, R', R'', \ldots)$ contenant ou non $V_{\nu-1}$ et V_ν, et ainsi de suite.

On peut donc représenter la formation d'une fonction algébrique x_1 telle que celle dont nous avons parlé par la chaîne suivante d'équations :

$$(2)\qquad \begin{aligned} V_\nu^{p_\nu} &= F_\nu(R', R'' \ldots), \\ V_{\nu-1}^{p_{\nu-1}} &= F_{\nu-1}(V_\nu, R', R'', \ldots), \\ V_{\nu-2}^{p_{\nu-2}} &= F_{\nu-2}(V_{\nu-1}, V_\nu, R', R'', \ldots), \\ &\ldots\ldots\ldots\ldots\ldots, \\ V_1^{p_1} &= F_1(V_2, V_3, \ldots V_\nu, R', R'', \ldots), \\ x_1 &= F_0(V_1, V_2, \ldots V_\nu, R', R'', \ldots), \end{aligned}$$

où les fonctions F sont rationnelles et les nombres p premiers absolus.

65. Nous allons montrer comment on peut simplifier la forme des fonctions F, mais nous commencerons par démontrer un théorème fondamental dont nous ferons souvent application.

THÉORÈME. — *Si les équations*

$$(3)\qquad f_1 x^{p-1} + f_2 x^{p-2} + \cdots + f_p = 0,$$

$$(4)\qquad x^p - F = 0$$

où p est premier, sont satisfaites simultanément, ou bien

$$f_1 = f_2 = \ldots = f_p = 0,$$

ou bien l'une des racines de l'équation (4) *s'exprime rationnellement au moyen de* $f_1, f_2, \ldots, f_p$ *et* F (*).

En effet, supposons que les coefficients de l'équation (3) ne soient pas tous nuls ; les équations (3) et (4) devant être satisfaites simultanément, les premiers membres doivent avoir un plus grand commun diviseur

$$x^k + \varphi_1 x^{k-1} + \ldots + \varphi_k$$

dont les coefficients s'expriment rationnellement au moyen de F, $f_1, f_2, \ldots, f_p$; s'il est du premier degré, il donne, égalé à zéro, une racine de l'équation (4) exprimée rationnellement; s'il n'est pas du premier degré, et si x_1 est une des racines communes, les autres seront de la forme $x_1\omega^\alpha, x_1\omega^\beta, \ldots,$ où ω est une racine p^e de l'unité, et l'on aura en effectuant leur produit

$$\pm\,\varphi_k = x_1^k\,\omega^{\alpha+\beta+\cdots} = x_1^k\,\omega^\gamma;$$

mais on peut trouver deux nombres u et v tels que $ku + pv = 1$; alors, en élevant les deux membres extrêmes à la puissance u, on a

$$\pm\,\varphi_k^u = x_1^{1-pv}\omega^{\gamma u} = x_1\omega^{\gamma u}\mathrm{F}^{-v},$$

d'où

$$x_1\omega^{\gamma u} = \pm\,\varphi_k^u \mathrm{F}^v,$$

et le premier membre, qui est une racine particulière de l'équation (4), s'exprime rationnellement au moyen de F, $f_1, f_2, \ldots, f_p$. Le théorème se trouve ainsi démontré.

66. Cela posé, je vais montrer qu'on peut mettre les fonctions F de la chaîne d'équations (2) sous forme d'une fonction entière par rapport aux éléments V, avec des coefficients rationnels par rapport à R′, R″, ... Supposons par exemple que $\mathrm{F}_{\alpha-1}$ ne soit pas une fonction entière par rapport à $\mathrm{V}_\alpha, \mathrm{V}_{\alpha+1}, \ldots, \mathrm{V}_\nu$; on peut d'abord la mettre sous forme du quotient de deux polynomes entiers et écrire

$$\mathrm{F}_{\alpha-1} = \frac{\mathrm{G}_0 + \mathrm{G}_1\mathrm{V}_\alpha + \cdots}{\mathrm{H}_0 + \mathrm{H}_1\mathrm{V}_\alpha + \cdots},$$

(*) Abel (*Œuvres complètes*, t. II, p. 196) a énoncé le premier ce théorème; c'est Kronecker (*Monatsberichte*, 1879, p. 206) qui lui a donné sa signification précise.

où $G_0, G_1, \ldots, H_0, H_1, \ldots$ sont entiers par rapport à $V_{\alpha+1}, \ldots, V_\nu$, puis ramener le numérateur et le dénominateur à ne contenir que les puissances de V_α au plus égales à $p_\alpha - 1$ d'après l'équation

$$(5) \qquad V_\alpha^{p_\alpha} = F_\alpha(V_{\alpha+1}, \ldots, V_\nu, R', R'', \ldots).$$

Si V_α entre encore au dénominateur de $F_{\alpha-1}$, désignons par $V'_\alpha, V''_\alpha, \ldots$ les autres racines de l'équation précédente; elles satisfont à l'équation

$$(6) \qquad \frac{X^{p_\alpha} - V_\alpha^{p_\alpha}}{X - V_\alpha} = X^{p_\alpha - 1} + V_\alpha X^{p_\alpha - 2} + \cdots + V_\alpha^{p_\alpha - 1} = 0.$$

Le produit

$$\Pi = (H_0 + H_1 V'_\alpha + \cdots)(H_0 + H_1 V''_\alpha + \cdots)\cdots$$

n'est pas nul, car si l'un des facteurs l'était, une des racines $V'_\alpha, V''_\alpha, \ldots$ satisferait simultanément à l'équation (5) et à une équation de degré $p_\alpha - 1$ au plus dont les coefficients $H_0, H_1, \ldots$ ne sont pas tous nuls; d'après le théorème précédent, une des racines de l'équation (5) serait rationnellement exprimable au moyen de $V_{\alpha+1}, V_{\alpha+2}, \ldots, V_\nu, R', R'', \ldots$ et F_α serait une puissance $p_\alpha{}^e$ exacte, contrairement à l'hypothèse.

Multiplions alors les deux termes de $F_{\alpha-1}$ par le produit Π; le dénominateur est symétrique par rapport aux racines de l'équation (5) et s'exprime rationnellement au moyen de $V_{\alpha+1}, \ldots, V_\nu$; le numérateur est le produit d'un polynome entier par rapport à V_α et d'une fonction Π symétrique entière par rapport aux racines de l'équation (6) et s'exprimant par conséquent d'une manière entière par rapport à V_α. On obtient ainsi comme expression de $F_{\alpha-1}$ un polynome entier par rapport à V_α; si les coefficients sont fractionnaires par rapport à $V_{\alpha+1}$, on opérera de la même manière par rapport à cette quantité, et ainsi de suite, de sorte que $F_{\alpha-1}$ sera une fonction entière des éléments $V_\alpha, V_{\alpha+1}, \ldots, V_\nu$ avec des coefficients rationnels dans le domaine primitif.

Le calcul étant ainsi effectué de proche en proche à partir de F_ν, on peut supposer de plus que chaque élément tel que V_α entre à une puissance au plus égale à $p_\alpha - 1$, car sinon on utiliserait l'équation $V_\alpha^{p_\alpha} = F_\alpha$ pour exprimer les puissances supérieures de V_α; par ce calcul les fonctions F ne cessent pas d'être entières par rapport aux éléments qu'elles renferment. On peut donc écrire

$$F_{\alpha-1} = J_0 + J_1 V_\alpha + J_2 V_\alpha^2 + \cdots + J_{p_\alpha - 1} V_\alpha^{p_\alpha - 1},$$

où les J sont des fonctions entières de $V_{\alpha+1}, V_{\alpha+2}, \ldots, V_\nu$.

67. On peut aller plus loin dans cette réduction dans le cas où V_α entre effectivement dans l'expression précédente, et faire en sorte que le coefficient du terme du premier degré J_1 soit égal à l'unité.

Soit J_k un des coefficients $J_1, J_2, \ldots, J_{p_\alpha-1}$ qui ne soit pas nul ; posons

$$J_k V_\alpha^k = W_\alpha; \tag{7}$$

il existe deux nombres u et v dont le premier n'est pas nul, tels que

$$ku + p_\alpha v = 1;$$

alors, en élevant à la puissance u les deux membres de l'équation (7), on obtient

$$J_k^u V_\alpha^{1-p_\alpha v} = J_k^u V_\alpha F_\alpha^{-v} = W_\alpha^u,$$

d'où l'on tire

$$V_\alpha = W_\alpha^u F_\alpha^v J_k^{-u}; \tag{8}$$

les équations (7) et (8) montrent que V_α et W_α s'expriment rationnellement l'un par l'autre et par les éléments suivants :

$$V_{\alpha+1}, V_{\alpha+2}, \ldots,$$

de sorte que les deux domaines de rationalité

$$(V_\alpha, V_{\alpha+1}, \ldots, V_\nu, R', R'', \ldots), \qquad (W_\alpha, V_{\alpha+1}, \ldots, V_\nu, R', R'', \ldots)$$

sont équivalents ; d'autre part il n'existe aucune puissance de W_α inférieure à p_α qui s'exprime rationnellement dans le domaine $(V_{\alpha+1}, \ldots, V_\nu, \ldots)$, car si l'on avait par exemple

$$W_\alpha^q = \Phi(V_{\alpha+1}, \ldots, V_\nu, \ldots),$$

pour q inférieur à p_α, on aurait, en partant de l'équation (7),

$$J_k^q V_\alpha^{kq} = \Phi(V_{\alpha+1}, \ldots, V_\nu, \ldots),$$

et comme le produit des deux nombres k et q n'est pas divisible par le nombre premier p_α, on en conclurait qu'une puissance de V_α inférieure à p_α serait rationnellement exprimable, ce qui est impossible. Par contre, en élevant W_α à la puissance p_α, on a

$$W_\alpha^{p_\alpha} = J_k^{p_\alpha} F_\alpha^k = \Phi_\alpha(V_{\alpha+1}, \ldots, V_\nu, R', R'', \ldots);$$

on déduit de ce qui précède que W_α, comme V_α, est fourni par une équation binome de degré p_α dans le domaine $(V_{\alpha+1}, \ldots)$, et qu'on peut les remplacer l'un par l'autre dans la chaîne d'équa-

tions (2) ; dès lors on peut introduire dans $F_{\alpha-1}$ et dans les fonctions suivantes $F_{\alpha-2}, \dots F_1$, W_α à la place de V_α. Dans $F_{\alpha-1}$ on remplacera, en se servant de l'équation (8), $J_h V_\alpha^h$ par $J_h(F_\alpha^v J_k^{-u})^h W_\alpha^{uh}$; cette fonction est de la forme $L_{h'} W_\alpha^{h'}$, en désignant par h' le nombre compris entre 1 et p_α qui diffère de uh d'un multiple de p_α, et par $L_{h'}$ une fonction rationnelle de $V_{\alpha+1}, V_{\alpha+2}, \dots, V_\nu$ qu'on peut ramener à une fonction entière par rapport à ces quantités.

En remarquant que les nombres

$$uh \ (h = 1, 2, \dots, p_\alpha - 1)$$

ont pour restes positifs (mod. p) des nombres distincts de la suite $1, 2, \dots, p_\alpha - 1$ et que k est la seule valeur de h donnant pour reste 1, on voit que l'on a

$$F_\alpha = J_0 + W_\alpha + L_2 W_\alpha^2 + \dots + L_{p_\alpha - 1} W_\alpha^{p_\alpha - 1},$$

où $J_0, L_2, \dots, L_{p_\alpha - 1}$ peuvent être supposés entiers par rapport à $V_{\alpha+1}$, $V_{\alpha+2}, \dots, V_\nu$. Nous conserverons la forme d'équation

$$V_{\alpha-1}^{p_\alpha - 1} = F_{\alpha-1} = J_0 + V_\alpha + J_2 V_\alpha^2 + \dots + J_{p_\alpha - 1} V_\alpha^{p_\alpha - 1}$$

en remplaçant W_α par la lettre V_α, et nous supposerons désormais que la réduction précédente ait été effectuée pour toutes les fonctions V ; nous aurons en particulier

$$x_1 = G_0 + V_1 + G_2 V_1^2 + \dots + G_{p_1 - 1} V_1^{p_1 - 1}.$$

68. Nous allons appliquer ce qui précède à l'expression algébrique qui satisfait identiquement à une équation résoluble. Supposons qu'elle soit fournie par la chaîne d'équations (2), où les fonctions F ont la forme que nous venons d'indiquer ; formons les différentes puissances de x_1 en ayant soin de réduire les exposants de $V_1, V_2, \dots$ à être inférieurs respectivement à $p_1, p_2, \dots$ au moyen des équations de la chaîne, et substituons-les dans le polynome $f(x)$; nous aurons le résultat

$$(9) \qquad f(x_1) = H_0 + H_1 V_1 + H_2 V_1^2 + \dots + H_{p_1 - 1} V_1^{p_1 - 1},$$

où $H_0, H_1, \dots, H_{p_1 - 1}$ sont des fonctions entières de $V_2, V_3, \dots, V_\nu$; il doit être identiquement nul.

D'après les hypothèses faites sur les fonctions F, cela ne peut avoir lieu que si l'on a $H_0 = H_1 = \dots = H_{p_1 - 1} = 0$, car sinon l'équation obtenue en annulant le polynome précédent entier en V_1 et l'équation

$$V_1^{p_1} = F_1(V_2, V_3, \dots, V_\nu, R', R'', \dots)$$

seraient satisfaites simultanément, et, d'après le théorème préliminaire, F_1 serait la puissance p_1^e exacte d'une fonction du domaine $(V_2, V_3, \ldots)$, ce qui est contraire à l'hypothèse.

De la même manière, chaque fonction H mise sous forme d'un polynome entier par rapport à V_2, avec des coefficients entiers par rapport à $V_3, V_4, \ldots$, tel que

$$H_i = K_0 + K_1 V_2 + K_2 V_2^2 + \cdots + K_{p_2-1} V_2^{p_2-1},$$

doit avoir ses coefficients $K_0, K_1, \ldots, K_{p_2-1}$ nuls pour une raison analogue, et ainsi de suite.

S'il arrive, dans quelques cas particuliers, que certains des polynomes successifs, ordonnés suivant l'élément V de moindre indice qu'ils renferment, n'aient pas tous leurs coefficients nuls, c'est une preuve que l'on a négligé de s'assurer que chaque fonction F n'est pas une puissance exacte, et qu'il est possible de réduire le nombre des éléments V.

Comme exemple d'une telle réduction, considérons l'équation du troisième degré $x^3 + px + q = 0$, et l'expression algébrique d'une racine x_1 donnée par la formule de Cardan

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}};$$

elle est fournie par la chaîne d'équations :

$$V_3^2 = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3,$$

$$V_2^3 = -\frac{q}{2} + V_3,$$

$$V_1^3 = -\frac{q}{2} - V_3,$$

$$x_1 = V_1 + V_2.$$

En substituant x_1 dans le premier membre de l'équation, on a

$$(V_1 + V_2)^3 + p(V_1 + V_2) + q = -q + 3V_1^2 V_2 + 3V_1 V_2^2 + pV_1 + pV_2 + q = 0;$$

les coefficients de V_1^2, V_1, et le terme indépendant ne sont pas identiquement nuls; ceci nous prouve que les fonctions V ne sont pas réduites au nombre minimum, et que V_1 fait partie du domaine (V_2, V_3, p, q) ; on obtiendra son expression, d'après la démonstra-

tion du théorème fondamental, en cherchant le plus grand commun diviseur des polynomes

$$3V_1^2V_2 + (3V_2^2 + p)V_1 + pV_2,$$

$$V_1^3 + \frac{q}{2} + V_3$$

et l'égalant à zéro, ou en remarquant que $(3V_1V_2 + p)(V_1 + V_2)$ doit être nul ; on trouve ainsi $V_1V_2 = -\frac{p}{3}$, ce qui donne

$$V_1 = \frac{-\frac{p}{3}}{V_2} = \frac{-\frac{p}{3}V_2^2}{-\frac{q}{2} + V_3} = \frac{V_2^2\left(-\frac{q}{2} - V_3\right)}{\left(\frac{p}{3}\right)^2};$$

nous avons fait disparaître successivement les irrationnelles du dénominateur, comme nous l'avons indiqué précédemment (§ 66); il résulte de là que la chaîne d'équations se réduit à

$$V_3^2 = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3,$$

$$V_2^3 = -\frac{q}{2} + V_3,$$

$$x_1 = V_2 + \frac{\left(-\frac{q}{2} - V_3\right)V_2^2}{\left(\frac{p}{3}\right)^2}.$$

69. Lorsque les éléments V sont réduits au nombre minimum, on a forcément, dans l'identité (9), $H_0 = H_1 = \cdots = H_{p_1-1} = 0$; supposons que, dans l'expression de x_1, on attribue à V_1 chacune des p_1 valeurs dont cette quantité est susceptible, et qui sont

$$V_1, \qquad \omega_1 V_1, \qquad \omega_1^2 V_1, \qquad \ldots, \qquad \omega_1^{p_1-1}V_1,$$

où ω_1 est une racine primitive de l'équation $\omega^{p_1} - 1 = 0$; on obtiendra des expressions $x_1, x_2, \ldots, x_{p_1}$ telles que

$$(10) \quad x_{k+1} = G_0 + \omega_1^k V_1 + G_2\omega_1^{2k}V_1^2 + \cdots (k = 0, 1, \ldots, p_1 - 1)$$

et en les substituant dans $f(x)$, on aura

$$f(x_{k+1}) = H_0 + H_1\omega_1^k V_1 + H_2\omega_1^{2k}V_2 + \cdots = 0;$$

car $H_0, H_1, \ldots$ sont nuls, par suite les p_1 quantités $x_1, x_2, \ldots, x_{p_1}$ sont

racines de l'équation proposée. Ainsi dans l'exemple de l'équation du troisième degré dont nous venons de parler, V_2 étant le dernier élément de la chaîne, les quantités

$$x_2 = \omega V_2 + \frac{\left(-\frac{q}{2} - V_3\right)\omega^2 V_2^2}{\left(\frac{p}{3}\right)^2},$$

$$x_3 = \omega^2 V_2 + \frac{\left(-\frac{q}{2} - V_3\right)\omega V_2^2}{\left(\frac{p}{3}\right)^2}$$

sont, avec x_1, des racines de l'équation.

70. Nous verrons que les racines ainsi formées sont distinctes, mais nous pouvons, sans le supposer, démontrer une propriété fondamentale des irrationnelles $V_1, V_2, \ldots, V_\nu$.

Les équations (10) donnent, en multipliant x_{k+1} par ω_1^{-k} et faisant la somme des produits,

$$p_1 V_1 = \Sigma \omega_1^{-k} x_{k+1},$$

(11) $$V_1 = \frac{1}{p_1} \Sigma_k \omega_1^{-k} x_{k+1} ;$$

par suite l'irrationnelle V_1 est une fonction linéaire des racines de l'équation $f(x) = 0$, les coefficients dépendant des racines p_1^{es} de l'unité; si les valeurs $x_1, x_2, \ldots, x_{p_1}$ fournies par les équations (10) ne sont pas toutes distinctes, on a par exemple

$$\Sigma_k \omega_1^{-k} x_{k+1} = x_1(1 + \omega_1^{-\alpha} + \ldots) + x_2(\omega_1^{-\beta} + \omega_1^{-\gamma} + \ldots) + \ldots$$

Soient $x_1, x_2, \ldots, x_n$ les n racines de l'équation donnée, qui sont toutes distinctes d'après l'hypothèse ; effectuons dans la somme précédente toutes les substitutions relatives à ces n racines, et lui donnant des valeurs algébriquement différentes ; toute fonction symétrique de ces valeurs est symétrique par rapport à $x_1, x_2, \ldots, x_n$; elle peut encore contenir la racine de l'unité ω_1 ; dans ce cas, si l'on remplace ω_1 par $\omega_1^2, \omega_1^3, \ldots, \omega_1^{p_1-1}$ et si l'on forme le produit des résultats, on aura une fonction symétrique s'exprimant rationnellement au moyen des coefficients de $f(x)$, c'est-à-dire au moyen des éléments $R', R'', \ldots$ du domaine primitif de rationalité.

En particulier, formons le produit des expressions obtenues en

effectuant dans

$$y - \left[\frac{1}{p_1}\Sigma\omega_1^{-k}x_{k+1}\right]^{p_1}$$

les substitutions précédentes par rapport aux racines x, et, s'il est nécessaire, multiplions ce produit par ceux que l'on obtient en remplaçant ω_1 par les autres racines de l'unité ; nous obtenons un polynome $\varphi(y)$ à coefficients rationnels par rapport à R', R'', ... En l'égalant à zéro, on a une équation analogue à $f(x) = 0$, et l'on peut supposer que ses racines sont distinctes, car sinon on lui appliquerait la méthode de calcul des racines égales qui ne change pas la nature des coefficients ; si nous admettons que $\varphi(y) = 0$ soit l'équation ainsi obtenue, sans racines égales, elle a en particulier pour racine la quantité

$$y_1 = \left[\frac{1}{p_1}\Sigma\omega_1^{-k}x_{k+1}\right]^{p_1} = V_1^{p_1} = F_1(V_2, V_3, \ldots);$$

elle est, comme on sait, de la forme

$$y_1 = L_0 + L_1V_2 + L_2V_2^2 + \cdots + L_{p_2-1}V_2^{p_2-1},$$

où L_1 est égal à l'unité. En répétant sur y_1 le raisonnement que nous avons fait sur x_1, les valeurs

$$(12)\quad y_{k+1} = L_0 + L_1\omega_2^kV_2 + L_2\omega_2^{2k}V_2^2 + \cdots + L_{p_2-1}\omega_2^{(p_2-1)k}V_2^{p_2-1}$$

pour $k = 0, 1, 2, \ldots, p_2 - 1$, où ω_2 est une racine p_2^e de l'unité, sont toutes des racines de $\varphi(y) = 0$; d'après la manière dont nous avons obtenu cette dernière équation, ce sont donc des fonctions des racines x analogues à y_1, et s'en déduisant par certaines substitutions effectuées sur $x_1, x_2, \ldots, x_n$. Si nous opérons comme nous l'avons fait pour V_1, nous avons

$$V_2 = \frac{1}{p_2}\Sigma_k\omega_2^{-k}y_{k+1},$$

de sorte que V_2 est une fonction entière des racines de $f(x) = 0$, avec des coefficients dépendant des racines de l'unité ω_1 et ω_2.

En répétant sur les racines y le même raisonnement, on formera une nouvelle équation $\psi(z) = 0$ dont les coefficients font partie du domaine primitif et dont les racines sont fonctions entières de $x_1, x_2, \ldots, x_n$, et l'on exprimera V_3 au moyen de ces racines, et ainsi de suite, d'où le théorème suivant :

THÉORÈME. — *Si une équation résoluble $f(x) = 0$ dont les coeffi-*

cients font partie d'un domaine de rationalité $(R', R'', \ldots)$, *est satisfaite par une expression algébrique explicite* x_1, *cette expression peut se mettre sous la forme d'une fonction entière d'une série de quantités*

$$V_1, V_2, \ldots, V_\nu,$$

avec des coefficients rationnels dans le domaine $(R', R'', \ldots)$. *Les quantités* V *sont d'une part des fonctions entières des racines de l'équation donnée, avec des coefficients dépendant de racines de l'unité ; d'autre part elles sont déterminées par une série d'équations de la forme*

$$V_\alpha^{p_\alpha} = F_\alpha(V_{\alpha+1}, \quad V_{\alpha+2}, \ldots, \quad V_\nu, R', R'', \ldots),$$

où les nombres p_α *sont premiers, et où les fonctions* F *sont entières par rapport aux quantités* V *qu'elles renferment, avec des coefficients rationnels dans le domaine* $(R', R'', \ldots)$.

71. Ce théorème permet d'appliquer les considérations que nous avons développées sur les fonctions des racines d'une équation, et nous allons démontrer le théorème fondamental suivant :

Théorème. — *Les équations générales de degré supérieur à quatre ne sont pas résolubles algébriquement.*

Soit

$$f(x) = x^n + c_1x^{n-1} + \ldots + c_n = 0$$

l'équation générale de degré n ; le domaine de rationalité est constitué par les coefficients $c_1, c_2, \ldots, c_n$ qui sont arbitraires et indépendants, et les racines $x_1, x_2, \ldots, x_n$ ne sont assujetties à aucune autre condition qu'à celle d'avoir leurs fonctions symétriques connues.

La racine x_1 étant supposée exprimée au moyen des quantités $V_1, V_2, \ldots, V_\nu$, comme nous l'avons dit, la dernière irrationnelle satisfait à une équation de la forme

$$V_\nu^{p_\nu} = F_\nu(c_1, c_2, \ldots, c_n);$$

elle est par suite une fonction entière des racines

$$V_\nu = \varphi(x_1, x_2, \ldots, x_n)$$

dont la puissance p_ν^e est symétrique.

L'identité $\quad \varphi^{p_\nu}(x_1, x_2, \ldots, x_n) = F_\nu(c_1, c_2, \ldots, c_n)$

a lieu lorsqu'on remplace $c_1, c_2, \ldots, c_n$ par leurs expressions en fonction des racines et lorsqu'on considère ensuite $x_1, x_2, \ldots, x_n$ comme des variables indépendantes, puisque l'équation est géné-

rale ; le second membre est invariable pour toute substitution ; par suite le premier doit l'être aussi ; mais φ change au moins pour une transposition, car sinon F_ν serait la puissance p_ν^e exacte d'une fonction symétrique, rationnelle par rapport à $c_1, c_2, \ldots, c_n$, contrairement à l'hypothèse.

Soit donc $T = (x_1 x_2)$ une transposition changeant la valeur de φ ; comme φ^{p_ν} reste invariable, la nouvelle valeur $\varphi(x_2, x_1, \ldots, x_n)$ ne diffère de la première que par une racine $p_\nu{}^e$ de l'unité ω_ν, de sorte que

$$\varphi(x_2, x_1, \ldots, x_n) = \omega_\nu \varphi(x_1, x_2, \ldots, x_n) ;$$

en répétant la transposition T sur les deux membres, ils resteront encore identiques puisque les x sont indépendants ; mais le premier reprend la valeur primitive $\varphi(x_1, x_2, \ldots, x_n)$; on a dès lors

$$\varphi(x_1, x_2, \ldots, x_n) = \omega_\nu \varphi(x_2, x_1, \ldots, x_n),$$

d'où, en remplaçant $\varphi(x_2, x_1, \ldots)$ par sa valeur,

$$\varphi(x_1, x_2, \ldots, x_n) = \omega_\nu^2 \varphi(x_1, x_2, \ldots, x_n) ;$$

cette identité exige que l'on ait $\omega_\nu^2 = 1$, d'où $p_\nu = 2$. On voit que la première irrationnelle V_ν que l'on a à calculer est un radical carré ; c'est une fonction des racines ayant deux valeurs, et appartenant au groupe alterné ; elle est le produit d'une fonction symétrique par la racine carrée du discriminant.

Passons maintenant à l'irrationnelle suivante $V_{\nu-1}$, donnée par

$$V_{\nu-1}^{p_{\nu-1}} = F_{\nu-1}(V_\nu, c_1, c_2, \ldots, c_n).$$

Le second membre doit renfermer V_ν, car sinon, d'après le même raisonnement $V_{\nu-1}$ serait encore une fonction de $x_1, x_2, \ldots, x_n$ ayant deux valeurs, appartenant au groupe alterné, et s'exprimerait rationnellement au moyen de V_ν, $c_1, c_2, \ldots, c_n$, contrairement à l'hypothèse.

Si l'on remplace $V_\nu, c_1, c_2, \ldots, c_n$ par leurs valeurs en fonction des racines, $F_{\nu-1}$ est une fonction appartenant au groupe alterné, et si l'on pose

$$V_{\nu-1} = \psi(x_1, x_2, x_3, \ldots, x_n),$$

$V_{\nu-1}$ est une fonction des variables x dont la puissance $p_{\nu-1}{}^e$ a deux valeurs et reste invariable pour les substitutions de ce groupe. ψ varie au moins pour une substitution circulaire de trois éléments, car sinon, d'après le § 5, elle appartiendrait au groupe alterné, et

$V_{\nu-1}$ s'exprimerait rationnellement au moyen de V_ν, ce qui est impossible.

Soit alors, par exemple, $S = (x_1x_2x_3)$ une substitution qui transforme ψ en une fonction que je désigne par ψ_1 ; elle changera ψ_1 en une nouvelle valeur ψ_2 et ψ_2 en ψ, puisque $S^3 = 1$. Comme S fait partie du groupe alterné, elle laisse invariable la valeur de $F_{\nu-1}$, et l'on a $\psi_1^{p_{\nu-1}} = \psi^{p_{\nu-1}}$, d'où

$$\psi_1 = \omega_{\nu-1}\psi,$$

$\omega_{\nu-1}$ désignant une racine $p^e_{\nu-1}$ de l'unité ; alors en répétant deux fois la substitution S on a

$$\psi_2 = \omega_{\nu-1}\psi_1 = \omega^2_{\nu-1}\psi,$$

$$\psi = \omega_{\nu-1}\psi_2 = \omega^3_{\nu-1}\psi\,;$$

par suite $\omega^3_{\nu-1} = 1$, $p_{\nu-1} = 3$, et la deuxième irrationnelle doit être un radical cubique.

Mais si le nombre des variables est > 4, ψ varie au moins pour une substitution circulaire de cinq éléments, d'après les propriétés du groupe alterné; si S′ est une telle substitution, un raisonnement identique au précédent montre que l'on doit avoir

$$\omega^5_{\nu-1} = 1, \qquad p_{\nu-1} = 5.$$

Il y a donc contradiction avec ce qui précède, et la résolution algébrique est impossible pour $n \geqslant 5$. On voit que pour $n = 3$ ou 4 le premier radical est la racine carrée du discriminant, et le second un radical cubique, ce que nous avons constaté.

72. Ce théorème fondamental a été démontré pour la première fois par Abel ; la démonstration qui précède est celle qu'a donnée Wantzel. Nous aurions pu nous en dispenser et nous appuyer sur les résultats déjà obtenus, mais nous avons préféré donner une théorie complète en elle-même de la résolution algébrique des équations générales.

Nous allons indiquer une autre démonstration. Nous avons vu aux § **24** et **25** que les fonctions alternées de plusieurs variables indépendantes sont les seules dont les valeurs conjuguées soient racines d'une équation binome à coefficients symétriques, et qu'il n'existe, pour $n > 4$, aucune fonction ayant m valeurs pour les substitutions du groupe alterné, et dont les m valeurs conjuguées soient racines d'une équation binome.

Il pourrait se faire cependant qu'une des valeurs conjuguées, en particulier, soit racine d'une équation binome à laquelle ne satisfont pas les autres. Je vais montrer d'abord que, dans le cas de l'équation générale, il n'y a que les fonctions alternées des racines dont une puissance de degré premier soit symétrique.

Soit, en effet, $\varphi_1(x_1, x_2, \ldots, x_n)$ une fonction ayant ρ valeurs conjuguées, racines d'une équation

$$(13) \qquad \Phi(\varphi) = \varphi^\rho + A_1\varphi^{\rho-1} + \cdots + A_\rho = 0$$

à coefficients symétriques, et satisfaisant à une équation binome telle que

$$(14) \qquad \varphi^p = F(c_1, c_2, \ldots, c_n).$$

Si les équations précédentes sont identiques, les ρ valeurs conjuguées sont les racines de l'équation binome (14) ; cela ne peut avoir lieu que si $\rho = p = 2$, et alors φ_1 est une fonction alternée ; si elles ne le sont pas, p ne peut être inférieur à ρ, car l'équation (13) est irréductible (§ 49) ; les racines communes satisfont alors à une équation de degré inférieur à p, de la forme

$$(15) \qquad B_1\varphi^{p-1} + B_2\varphi^{p-2} + \cdots + B_p = 0$$

à coefficients symétriques, mais c'est impossible, car d'après le théorème préliminaire de ce chapitre, φ_1 serait symétrique.

On démontrerait de la même manière qu'il n'existe, pour $n > 4$, aucune fonction des racines de l'équation générale dont une puissance de degré premier soit une fonction alternée. Le théorème d'Abel en découle immédiatement.

73. Revenons aux équations spéciales résolubles algébriquement, pour compléter ce que nous avons dit au sujet de leurs racines.

Nous avons vu que les expressions

$$(10) \qquad x_{k+1} = G_0 + G_1\omega_1^k V_1 + \cdots + G_{p_1-1}\omega_1^{k(p_1-1)}V_1^{p_1-1}$$

obtenues en remplaçant dans x_1 V_1 par $\omega_1^k V_1$, et où G_1 peut être supposé égal à l'unité, donnent des racines de l'équation $f(x) = 0$; nous pouvons généraliser, et démontrer le théorème suivant :

THÉORÈME. — *Si dans l'expression de la racine satisfaisant à une équation résoluble*

$$x_1 = G_0(V_2, V_3, \ldots) + G_1(V_2, V_3, \ldots)V_1 + \cdots + G_{p_1-1}V_1^{p_1-1}$$

on remplace une ou plusieurs des irrationnelles par une autre des va-

leurs dont elles sont susceptibles, on a une nouvelle racine de l'équation.

En effet, nous avons vu que dans le résultat de substitution

$$f(x_1) = H_0(V_2, V_3, \ldots) + H_1(V_2, V_3, \ldots)V_1 + \cdots + H_{p_1-1}V_1^{p_1-1}$$

chacun des coefficients $H_0, H_1, \ldots, H_{p_1-1}$ doit être nul identiquement, et de même, si on les ordonne suivant les puissances de V_2, les coefficients de ces puissances doivent être nuls, et ainsi de suite.

Nous avons déjà vu que si l'on remplace V_1 par $\omega_1^k V_1$, on forme des racines de $f(x) = 0$.

Supposons maintenant que l'on remplace V_2 par $V_2' = \omega_2 V_2$, où ω_2 est une racine de $\omega^{p_2} - 1 = 0$; V_1 doit être alors remplacé par une racine V_1' de l'équation

$$V_1'^{p_1} = F_1(V_2', V_3, \ldots, V_\nu, R', R'', \ldots).$$

$F_1(V_2, V_3, \ldots)$ n'était pas la puissance p_1^e exacte d'une fonction du domaine $(V_2, V_3, \ldots)$; par suite $F_1(V_2', V_3, \ldots)$ n'est pas non plus la puissance exacte d'une fonction du nouveau domaine $(V_2', V_3, \ldots)$ et la suite

$$V_\nu, V_{\nu-1}, \ldots, V_3, V_2', V_1'$$

jouit des mêmes propriétés que la suite primitive ; si l'on remplace dans x_1 V_2 et V_1 par V_2' et V_1', la nouvelle valeur

$$x_1' = G_0(V_2', V_3, \ldots) + G_1(V_2', V_3, \ldots)V_1' + \cdots$$

est encore racine de l'équation, car $f(x_1')$ est identiquement nul.

La démonstration s'étend de proche en proche à toutes les irrationnelles.

74. Les racines que l'on obtient ainsi ne sont pas toujours distinctes; nous allons reconnaître celles qui le sont, en supposant toujours l'équation donnée irréductible.

Considérons d'abord les racines $x_1, x_2, \ldots, x_{p_1}$ données par les équations (10) ; je vais montrer qu'elles sont distinctes. Le produit

$$f_1(x) = (x - x_1)(x - x_2)\ldots(x - x_{p_1})$$

est symétrique par rapport à $V_1, \omega_1 V_1, \omega_1^2 V_1, \ldots,$ par suite s'exprime rationnellement dans le domaine $(V_2, V_3, \ldots)$; je dis qu'il est irréductible dans ce domaine.

Supposons qu'il ne le soit pas, et qu'il se décompose dans les

facteurs irréductibles

$$\varphi_1(x, V_2, V_3, \ldots) = (x - x_1)(x - x_\alpha) \ldots,$$
$$\varphi_2(x, V_2, V_3, \ldots) = (x - x_\beta)(x - x_\gamma) \ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots;$$

les premiers membres ne renfermant pas V_1, cette irrationnelle doit disparaître identiquement dans les seconds après tous produits effectués, dès lors ils ne changeront pas lorsqu'on remplacera V_1 par $\omega_1 V_1$, ..., c'est-à-dire x_1 par chacune des autres racines ; il faut donc que les facteurs irréductibles φ_1, φ_2, ... soient identiques, c'est-à-dire que $f_1(x)$ soit une puissance exacte ; mais, comme p_1 est un nombre premier, $f_1(x)$ ne peut être puissance exacte que d'un facteur du premier degré qui serait $x - x_1$, et cela est impossible puisque $x - x_1$ n'est pas rationnel par rapport à V_2, V_3, ...

De ce que $f_1(x)$ est irréductible, on déduit que $x_1, x_2, \ldots, x_{p_1}$ sont distinctes, ce que nous voulions démontrer ; on peut ajouter que $f_1(x)$ est un facteur irréductible de $f(x)$ dans le domaine $(V_2, V_3, \ldots)$.

Il arrive généralement que dans le produit $(x - x_1)(x - x_2) \ldots (x - x_{p_1})$ plusieurs irrationnelles disparaissent en même temps que V_1 ; supposons que $V_2, V_3, \ldots$ disparaissent, jusqu'à V_{h-1}, et que V_h soit l'irrationnelle de moindre indice qui subsiste ; on a alors

$$f(x, R', R'', \ldots) = f_1(x, V_h, V_{h+1}, \ldots)\psi_1(x, V_h, V_{h+1}, \ldots),$$

et l'on peut supposer que le quotient ψ_1 ait été rendu entier par rapport aux éléments V qu'il contient.

L'identité précédente montre que les coefficients des puissances de x doivent être identiques aux deux membres ; ceux du second membre, ordonnés suivant les puissances $V_h^0, V_h^1, V_h^2, \ldots, V_h^{p_h - 1}$, doivent avoir les coefficients de ces puissances séparément nuls, d'après un raisonnement déjà fait, et l'identité précédente subsistera quand on remplacera V_h par $\omega_h^k V_h$, où $\omega_h^{p_h} - 1 = 0$.

Formons maintenant le produit des p_h facteurs obtenus en remplaçant dans f_1 V_h par toutes les valeurs dont cette irrationnelle est susceptible,

$$f_2(x) = f_1(x, V_h, \ldots) f_1(x, \omega_h V_h, \ldots) f_1(x, \omega_h^2 V_h, \ldots) \ldots;$$

je vais montrer qu'il est irréductible dans le domaine formé par $(V_{h+1}, V_{h+2}, \ldots)$; supposons en effet qu'il ne le soit pas, et que

$$\varphi_1(x, V_{h+1}, \ldots)$$

soit un facteur irréductible dans ce domaine ; s'il a un diviseur commun avec un des facteurs précédents, par exemple avec $f_1(x, \omega_h^k V_h, V_{h+1}, \ldots)$, il doit être divisible par ce polynome, car sinon celui-ci serait réductible dans le domaine $(\omega_h^k V_h, V_{h+1}, \ldots)$ et $f_1(x, V_h, V_{h+1}, \ldots)$ le serait aussi dans le domaine $(V_h, V_{h+1}, \ldots)$, ce qui est impossible. Il faut donc que φ_1 soit le produit d'un certain nombre de facteurs f_1 ; soient alors

$$\varphi_1(x, V_{h+1}, \ldots) = f_1(x, V_h, V_{h+1}, \ldots) f_1(x, \omega_h^2 V_h, V_{h+1}, \ldots) \ldots,$$

$$\varphi_2(x, V_{h+1}, \ldots) = f_1(x, \omega_h^\beta V_h, V_{h+1}, \ldots) f_1(x, \omega_h^\gamma V_h, V_{h+1}, \ldots) \ldots,$$

. . . .

les facteurs irréductibles de $f_2(x)$; V_h doit disparaître dans les seconds membres quand on effectue les produits. La première identité ne changeant pas quand on remplace V_h par $\omega_h^k V_h$, on en conclut que les facteurs $\varphi_1, \varphi_2, \ldots$ sont identiques et que $f_2(x)$ est une puissance exacte d'un polynome dont le degré est de la forme λp_1 ; comme p_h est premier, cela ne peut avoir lieu que si $f_2(x)$, dont le degré est égal à $p_1 p_h$, est la puissance p_h^e d'un facteur qui ne peut être que $f_1(x, V_h, V_{h+1}, \ldots)$; mais cela est impossible, puisque f_1 contient sûrement V_h et n'est pas rationnel en $V_{h+1}, V_{h+2}, \ldots, V_\nu$.

Ainsi donc $f_2(x)$ est irréductible dans le domaine $(V_{h+1}, V_{h+2}, \ldots)$; par suite les $p_1 p_h$ racines qu'on obtient en remplaçant dans $x_1, x_2, \ldots, x_{p_1}$ V_h par les expressions de la forme $\omega_h^k V_h$ sont distinctes, et $f_2(x)$ est un facteur de $f(x)$; on peut ajouter que s'il existe entre V_1 et V_h des irrationnelles $V_2, V_3, \ldots, V_{h-1}$ ayant disparu dans $f_1(x, V_h, \ldots)$, toutes les expressions qu'on obtiendrait en remplaçant V_2 par $\omega_2^k V_2$, V_3 par $\omega_3^k V_3, \ldots, V_{h-1}$ par $\omega_{h-1}^k V_{h-1}$ ne peuvent donner de nouvelles racines de $f(x)$, car elles satisfont forcément à l'équation $f_2(x) = 0$ et ne peuvent différer des $p_1 p_h$ racines que nous venons de trouver.

En continuant de la même manière, supposons que dans $f_2(x)$, en même temps que V_h disparaissent d'autres irrationnelles V_{h+1}, $V_{h+2}, \ldots, V_{k-1}$, et que V_k soit la première qui subsiste ; formons le produit

$$f_3(x) = f_2(x, V_k, V_{k+1}, \ldots) f_2(x, \omega_k V_k, V_{k+1}, \ldots) f_2(x, \omega_k^2 V_k, \ldots) \ldots ;$$

on verra que c'est un facteur irréductible de $f(x)$ dans le domaine $(V_{k+1}, V_{k+2}, \ldots)$, et ainsi de suite ; après un nombre limité d'opérations on fera disparaître toutes les irrationnelles et on obtiendra un

facteur irréductible de $f(x)$ dans le domaine $(R', R'', ...)$; comme $f(x)$ est supposé irréductible dans ce domaine, le dernier produit ne différera pas de ce polynome lui-même ; le raisonnement précédent montre de plus comment on obtient toutes les racines séparément.

On peut donc énoncer le théorème suivant :

Théorème. — *Etant donnée l'expression algébrique x_1, satisfaisant à une équation résoluble irréductible $f(x, R', R'', ...) = 0$ et formée au moyen des irrationnelles $V_1, V_2, ..., V_\nu$, les p_1 quantités $x_1, x_2, ..., x_{p_1}$ obtenues en substituant à V_1 dans x_1, les p_1 déterminations dont elle est susceptible : $V_1, \omega_1 V_1, ... \omega_1^{p_1-1} V_1$, sont des racines distinctes de l'équation donnée ; si l'on forme le produit*

$$f_1(x, V_h, V_{h+1}, \ldots) = (x - x_1)(x - x_2)\ldots(x - x_{p_1}) \qquad (h \geqslant 2)$$

et que V_h soit l'irrationnelle de moindre indice subsistant dans f_1, les $p_1 p_h$ quantités obtenues en remplaçant dans $x_1, x_2, ..., x_{p_1}$ V_h par les déterminations $V_h, \omega_h V_h, .., \omega_h^{p_h-1} V_h$ sont $p_1 p_h$ racines distinctes de l'équation donnée ; de même si l'on forme le produit des facteurs linéaires correspondant à ces racines,

$$f_2(x, V_k, V_{k+1}, ...) = f_1(x, V_h, ...) f_1(x, \omega_h V_h, ...) ... f_1(x, \omega_h^{p_h-1} V_h, ...),$$

où $k \geqslant h+1$, on en déduit $p_1 p_h p_k$ racines distinctes de $f(x)$, et ainsi de suite jusqu'à ce que les irrationnelles disparaissent ; on obtient ainsi le polynome $f(x, R', R'', ...)$ et toutes les racines de l'équation ; le degré de $f(x)$ est égal à $n = p_1 p_h p_k \ldots$, et de plus les polynomes $f_1, f_2, ...$ sont irréductibles dans le domaine des éléments qu'ils contiennent.

75. Remarque. — L'ordre dans lequel sont placées les irrationnelles $V_1, V_2, ...$ n'est pas toujours absolument fixé par la nature de l'expression algébrique ; supposons par exemple que $V_\alpha, V_{\alpha+1}, ..., V_{\beta-1}$ soient déterminés séparément au moyen des irrationnelles suivantes : $V_\beta, V_{\beta+1}, ..., V_\nu$ par des équations de la forme

$$V_k^{p_k} = F_k(V_\beta, V_{\beta+1}, \ldots, V_\nu, R', R'', \ldots) \quad (k = \alpha, \ \alpha+1, \ldots \ \beta-1),$$

on peut ranger les éléments $V_\alpha, ..., V_{\beta-1}$ dans un ordre quelconque.

Si cela se présente pour un certain nombre d'irrationnelles à partir de V_1, on peut placer l'une quelconque d'entre elles au premier rang dans la suite totale des éléments V ; nous dirons que

chacune d'elles forme un radical extérieur dans l'expression algébrique de la racine.

Considérons le cas d'une équation irréductible de degré premier p_1 résoluble algébriquement ; d'après ce que nous avons dit relativement au degré de cette équation, la première irrationnelle V_1 doit être donnée par une équation de degré p_1, et de plus le produit

$$f_1(x) = (x - x_1)(x - x_2)\ldots(x - x_{p_1})$$

doit être identique à $f(x)$, de sorte que les irrationnelles suivantes

$$V_2,\ V_3,\ \ldots,\ V_\nu$$

doivent disparaître avec V_1 ; on a donc le corollaire suivant :

Corollaire. — *Si une équation irréductible de degré premier est résoluble algébriquement, le radical extérieur* V_1 *a un indice égal au degré de l'équation, et si l'expression d'une racine est*

$$x_1 = G_0 + G_1 V_1 + \cdots + G_{p_1-1} V_1^{p_1-1},$$

le premier membre de l'équation est égal au produit des p_1 *facteurs*

$$f(x) = \prod_{k=0}^{k=p_1-1} \left[x - (G_0 + G_1 \omega_1^k V_1 + G_2 \omega_1^{2k} V_1^2 + \cdots + G_{p_1-1} \omega_1^{k(p-1)} V_1^{p_1-1})\right].$$

CHAPITRE X

DES ÉQUATIONS ABÉLIENNES

---

76. Considérons une équation irréductible $f(x) = 0$ jouissant de la propriété qu'une racine x'_1 soit une fonction rationnelle $\theta(x_1)$ d'une autre racine x_1 dans le domaine de rationalité ; nous allons montrer comment on peut simplifier la résolution de cette équation, et, dans certains cas, l'effectuer au moyen de radicaux.

Soit

$$(1) \qquad f(x) = 0$$

l'équation donnée, supposée irréductible,

$$(2) \qquad x'_1 = \theta(x_1)$$

la relation qui existe entre deux racines ; l'équation (1) et la suivante

$$(3) \qquad f[\theta(x)] = 0$$

ont en commun la racine x_1 ; d'après un théorème connu (§ 37), la dernière est satisfaite pour toutes les racines de la première, en particulier pour x'_1, de sorte que l'on a, en remplaçant x par x'_1 dans l'équation (3),

$$f[\theta(x'_1)] = f\{\theta[\theta(x_1)]\} = 0.$$

Représentons pour abréger par $\theta^2(x)$, $\theta^3(x)$, ... les fonctions

$$\theta[\theta(x)], \quad \theta[\theta^2(x)], \ldots ;$$

nous voyons, en répétant le raisonnement précédent, que les termes de la suite indéfinie

$$(4) \qquad x_1, \ \theta(x_1), \ \theta^2(x_1), \ldots$$

sont des racines de l'équation (1) ; comme celle-ci n'a qu'un nombre

limité de racines, on parviendra nécessairement, dans la suite que nous venons de former, à une fonction égale à l'une des précédentes ; soient $\theta^k(x_1)$ et $\theta^{m+k}(x_1)$ les deux premières qui soient égales ; on doit avoir $k = 0$, car sinon l'équation

$$\theta^m(x) - x = 0$$

serait satisfaite par la racine $\theta^k(x_1)$ de l'équation (1), par suite par toutes les racines et en particulier pour x_1 ; on aurait par conséquent

$$\theta^m(x_1) = x_1 ;$$

et k ne serait pas le plus petit nombre jouissant de la propriété énoncée. Soit alors m la plus petite valeur pour laquelle on ait $^m(x_1) = x_1$; on en conclut que x_1, $\theta(x_1)$, $\theta^2(x_1)$, ..., $\theta^{m-1}(x_1)$ sont distincts, et que les termes suivants de la suite (4) reproduisent périodiquement les m précédents.

Si m est égal au degré de l'équation, les racines sont toutes déterminées au moyen de x_1 ; si le degré n de $f(x)$ est supérieur à m, et si l'on représente par x_2 une racine distincte de celles dont nous venons de parler, l'équation (3) admet toutes les racines de $f(x) = 0$, en particulier x_2, par suite $\theta(x_2)$ est encore racine et l'on obtient de cette façon une deuxième série de racines,

(5) $$x_2, \theta(x_2), \theta^2(x_2), \ldots, \theta^{\mu-1}(x_1),$$

distinctes les unes des autres, et reproduites périodiquement par les termes suivants : $\theta^\mu(x_1)$, ...

On doit avoir $\mu = m$, car les équations

$$\theta^m(x) - x = 0, \qquad \theta^\mu(x) - x = 0$$

sont satisfaites par toutes les racines de l'équation irréductible $f(x)$, et en particulier, la première par x_2, la seconde par x_1 ; chacun des nombres m et μ est alors au moins égal à l'autre, de sorte qu'ils sont égaux.

De plus, les termes de la suite (5) sont tous différents de ceux de la suite (4), car si l'on avait par exemple

$$\theta^b(x_2) = \theta^a(x_1),$$

où a et b sont $< m$, on en déduirait, en appliquant aux deux membres l'opération θ^{m-b},

$$\theta^m(x_2) = x_2 = \theta^{m-b+a}(x_1),$$

de sorte que x_2 serait compris dans la suite (4), contrairement à l'hypothèse.

Si les $2m$ racines obtenues ne forment pas la totalité des racines de l'équation donnée, on répétera le raisonnement sur une nouvelle racine x_3, etc.; on obtient de cette façon les résultats suivants :

THÉORÈME. — *Si une racine d'une équation irréductible* $f(x) = 0$ *est une fonction rationnelle d'une autre, on peut ranger toutes les racines de cette équation en* ν *séries de* m *chacune, comme l'indique le tableau suivant :*

$$\begin{array}{l} x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots\ \theta^{m-1}(x_1), \\ x_2,\ \theta(x_2),\ \theta^2(x_2),\ \ldots\ \theta^{m-1}(x_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x_\nu,\ \theta(x_\nu),\ \theta^2(x_\nu),\ \ldots\ \theta^{m-1}(x_\nu). \end{array}$$

On a pour $\alpha = 1, 2, \ldots, \nu$

$$\theta^m(x_\alpha) = x_\alpha,$$

et le degré de l'équation est égal à $m\nu$.

77. Nous allons, dans le cas où le nombre ν des séries est supérieur à l'unité, ramener la résolution de l'équation donnée à celle de ν équations de degré m ayant respectivement pour racines celles de chacune des séries précédentes.

Nous commencerons par former le groupe de l'équation (1); d'après ce que nous avons dit au § 46, nous devons chercher un facteur irréductible de l'équation résolvante $\Psi(z)$ dont les racines sont les n ! valeurs de la fonction de Galois, ou bien encore chercher les facteurs linéaires de cette équation résolvante qu'il faut associer pour constituer un diviseur $\Psi_1(z)$ de $\Psi(z)$, à coefficients rationnels et irréductible.

Désignons par $S_1, S_2, \ldots, S_\nu$ les substitutions circulaires

$$\begin{array}{l} S_1 = [x_1\ \theta(x_1)\ \theta^2(x_1)\ \ldots], \\ S_2 = [x_2\ \theta(x_2)\ \theta^2(x_2)\ \ldots], \\ \ldots\ldots\ldots\ldots, \end{array}$$

dont les cycles sont constitués par les m racines de chacune des ν séries ; ces cycles n'ayant aucun élément commun, ces substitutions sont permutables et engendrent un groupe d'ordre m^ν.

Considérons maintenant les substitutions permutant entre elles les ν séries de racines de toutes les manières possibles, tout en

conservant l'ordre des éléments de chacune d'elles ; elles sont en même nombre que les substitutions du groupe symétrique des ν indices $1, 2, \ldots, \nu$, et nous les désignerons par $T_1, T_2, \ldots, T_{\nu!}$. Elles sont permutables aux substitutions circulaires précédentes, et le groupe G dérivé de $S_1, S_2, \ldots, T_1, T_2, \ldots$ a son ordre égal à $m^\nu.\nu\,!$; ainsi que nous le verrons plus loin (ch. XIII), ce groupe est non-primitif; nous allons montrer que c'est celui de l'équation $f(x) = 0$.

Prenons pour cela le facteur de l'équation résolvante de Galois

$$z - \psi_1 = z - [u_1 x_1 + u_2 \theta(x_1) + \cdots + u_{m+1} x_2 + u_{m+2} \theta(x_2) + \cdots]$$

et ceux qu'on en déduit en effectuant sur les n racines les substitutions du groupe précédent ; nous allons montrer que leur produit, qui est un polynome $\Psi_1(z)$ de degré $m^\nu.\nu\,!$, est rationnellement exprimable.

Si l'on prend d'abord les facteurs déduits de $z - \psi_1$ en effectuant les substitutions $1, S_1, S_1^2, \ldots, S_1^{m-1}$, leur produit p_1 est une fonction cyclique de $x_1, \theta(x_1), \ldots, \theta^{m-1}(x_1)$ et s'exprime rationnellement, en ce qui concerne ces racines, au moyen d'une fonction cyclique particulière C_1 appartenant numériquement au groupe dérivé de S_1 (§ 43). Cette fonction cyclique est une fonction rationnelle de x_1 ; mais comme le changement de x_1 en $\theta(x_1)$ a pour effet de remplacer en général $\theta^\alpha(x_1)$ par $\theta^{\alpha+1}(x_1)$ et $\theta^{m-1}(x_1)$ par $\theta^m(x_1) = x_1$, c'est-à-dire d'effectuer la substitution S_1, C_1 reste invariable lorsqu'on remplace x_1 par $\theta(x_1)$ et par chacune des autres racines de la même série, et l'on a

$$C_1(x_1) = C_1[\theta(x_1)] = \cdots = C_1[\theta^{m-1}(x_1)].$$

Si l'on prend ensuite les valeurs de p_1 pour la substitution S_2 et ses puissances, leur produit p_2 est, par rapport aux racines $x_2, \theta(x_2), \ldots, \theta^{m-1}(x_2)$ de la deuxième série, une fonction cyclique, et il s'exprime au moyen d'une fonction cyclique de ces racines ; on peut choisir une fonction C_2 déduite de C_1 en remplaçant x_1 par x_2 ; elle sera telle que l'on ait

$$C_2(x_2) = C_2[\theta(x_2)] = \cdots = C_2[\theta^{m-1}(x_2)].$$

En continuant de cette façon jusqu'à S_ν, on obtient un produit p_ν de degré m^ν, s'exprimant rationnellement au moyen de fonctions cycliques $C_1(x_1), C_2(x_2), \ldots, C_\nu(x_\nu)$ ne différant l'une de l'autre que par la notation des variables.

On effectue ensuite sur p_ν les substitutions $T_1, T_2, \ldots, T_{\nu!}$; le produit des résultats, qui est $\Psi_1(z)$, est un polynome en z dont les coefficients sont symétriques par rapport à $C_1, C_2, \ldots, C_\nu$; il reste à voir qu'ils s'expriment rationnellement.

Considérons pour cela la somme des puissances semblables de ces fonctions

$$\Sigma_\lambda = C_1^\lambda + C_2^\lambda + \cdots + C_\nu^\lambda ;$$

d'après ce que nous avons dit sur la fonction C_1, on a

$$mC^\lambda = C_1(x_1)^\lambda + C_1[\theta(x_1)]^\lambda + \cdots + C_1[\theta^{m-1}(x_1)]^\lambda,$$

et des égalités analogues relativement aux autres séries de racines ; on en conclut que $m\Sigma_\lambda$ est égal à la somme des valeurs de la fonction rationnelle $C_1(x_1)^\lambda$ lorsqu'on remplace x_1 par chacune des n racines de $f(x) = 0$; c'est dès lors une fonction symétrique de ces racines, s'exprimant rationnellement au moyen des coefficients de l'équation.

Comme cela a lieu pour toute valeur de λ, les sommes des puissances semblables, et par suite les fonctions symétriques de $C_1, C_2, \ldots, C_\nu$ sont exprimables rationnellement, ce que nous voulions démontrer.

Ainsi donc, la fonction $\Psi_1(z)$ est rationnelle ; comme on ne suppose d'autre part aucune relation entre les racines $x_1, x_2, \ldots, x_\nu$, il n'existe aucun produit de moindre degré jouissant de cette propriété. Celui que nous venons de déterminer constitue le premier membre de l'équation résolvante de Galois et le groupe est formé des substitutions dont nous avons parlé.

Si l'on applique à une fonction cyclique des racines de la première série, telle que $C_1[x_1, \theta(x_1), \ldots, \theta^{m-1}(x_1)]$, restant invariable par la substitution S_1 et ses puissances, les substitutions du groupe précédent, on voit qu'elle prend pour ces substitutions ν valeurs conjuguées, qui sont précisément les fonctions dont nous avons parlé

$$C_\alpha = C_1[x_\alpha), \theta(x_\alpha), \theta^2(x_\alpha), \ldots] \qquad (\alpha = 1, 2, \ldots, \nu) ;$$

ces ν valeurs sont les racines d'une équation,

$$(6) \qquad C^\nu + A_1 C^{\nu-1} + \cdots + A_\nu = 0,$$

dont les coefficients s'expriment rationnellement au moyen de ceux de $f(x)$; lorsqu'on connaît l'une des racines, par exemple celle qui correspond à la première série, les fonctions symétriques des m

racines de cette série restent invariables pour les substitutions qui n'altèrent pas C_1, et s'expriment rationnellement au moyen de cette fonction et des coefficients de $f(x)$.

Ainsi donc, en déterminant toutes les racines $C_1, C_2, \ldots, C_\nu$ d'une équation (6) de degré ν, on peut former ν équations distinctes de degré m,

$$f_\alpha(x) = x^m + a_1(C_\alpha)x^{m-1} + \ldots + a_m(C_\alpha) = 0 \qquad (\alpha = 1, 2, \ldots, \nu)$$

telles que les coefficients de l'équation $f_\alpha(x) = 0$ soient des fonctions rationnelles de la racine C_α et des coefficients de l'équation donnée $f(x) = 0$; les racines de l'équation de rang α sont

$$x_\alpha,\ \theta(x_\alpha),\ \theta^2(x_\alpha),\ \ldots,\ \theta^{m-1}(x_\alpha).$$

Si l'on ne fait sur les racines de l'équation (1) aucune autre hypothèse que celle dont nous avons parlé, les racines de l'équation (6) ne satisfont à aucune condition particulière, et la résolution de cette équation ne peut être simplifiée.

78. Nous supposons maintenant que l'on ait calculé une racine telle que C_1 de l'équation (6) et qu'on l'adjoigne au domaine de rationalité ; il nous reste à traiter ce problème : *Résoudre une équation* $f(x) = 0$, *de degré* m, *dont les racines sont distinctes et représentées par*

$$(7) \qquad x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots,\ \theta^{m-1}(x_1),$$

θ *étant une fonction rationnelle telle que* $\theta^m(x_1) = x_1$.

Considérons une fonction cyclique des racines, en particulier

$$T_1 = [x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \cdots + \omega^{m-1}\theta^{m-1}(x_1)]^m = \psi_1^m,$$

où ω est une racine primitive de l'équation $x^m - 1 = 0$; nous allons démontrer, sur la forme particulière de cette fonction, qu'elle est rationnellement exprimable ; en effet, si l'on change x_1 en $\theta(x_1)$, la fonction ψ_1 entre parenthèse se change en

$$\theta(x_1) + \omega\theta^2(x_1) + \omega^2\theta^3(x_1) + \cdots + \omega^{m-1}x_1 = \omega^{-1}\psi_1 ;$$

par suite T_1 conserve la même valeur ; il en est de même, en répétant le raisonnement, lorsqu'on remplace x_1 par une quelconque des racines ; si l'on pose alors pour un instant $T_1 = \varphi(x_1)$, on a

$$T_1 = \varphi(x_1) = \varphi[\theta(x_1)] = \cdots = \frac{1}{m}\,[\varphi(x_1) + \varphi[\theta(x_1)] + \cdots] ;$$

c'est une fonction symétrique des racines, et elle s'exprime rationnellement au moyen des coefficients de l'équation, lorsqu'on adjoint au domaine de rationalité les racines m^{es} de l'unité.

En extrayant une racine d'indice m, on a

$$\psi_1 = x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots + \omega^{m-1}\theta^{m-1}(x_1) = \sqrt[m]{T_1}\,;$$

ψ_1 est une fonction de Galois au moyen de laquelle on peut exprimer les racines, mais il est préférable de les déterminer de la manière suivante :

Supposons que l'on remplace dans ψ_1 la racine ω par chacune des racines de l'équation $x^m - 1 = 0$, qui sont

$$\omega,\ \omega^2,\ \omega^3,\ \ldots,\ \omega^{m-1},\ \omega^m = 1\,;$$

nous obtiendrons les fonctions

$$\psi_\alpha = x_1 + \omega^\alpha\theta(x_1) + \omega^{2\alpha}\theta(x_1) + \ldots + \omega^{(m-1)\alpha}\theta^{m-1}(x_1).$$

Elles s'expriment toutes en fonction rationnelle de ψ_1, car la fonction

$$\psi_\alpha\psi_1^{m-\alpha} = [x_1 + \omega^\alpha\theta(x_1) + \ldots][x_1 + \omega\theta(x_1) + \ldots]^{m-\alpha}$$

se transforme, par le changement de x_1 en $\theta(x_1)$, en

$$(\omega^{-\alpha}\psi_\alpha)(\omega^{-1}\psi_1)^{m-\alpha} = \psi_\alpha\psi_1^{m-\alpha}$$

et reste numériquement invariable ; d'après le raisonnement fait précédemment, elle s'exprime rationnellement au moyen des coefficients de l'équation ; si l'on représente par T_α cette fonction, on a $\psi_\alpha = \frac{T_\alpha}{T_1}(\sqrt[m]{T_1})^\alpha$, d'où la série d'équations :

$$x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \cdots = \sqrt[m]{T_1},$$

$$x_1 + \omega^2\theta(x_1) + \omega^4\theta^2(x_1) + \cdots = \frac{T_2}{T_1}(\sqrt[m]{T_1})^2,$$

. . . .

$$x_1 + \omega^{m-1}\theta(x_1) + \omega^{2(m-1)}\theta^2(x_1) + \cdots = \frac{T_{m-1}}{T_1}(\sqrt[m]{T_1})^{m-1},$$

$$x_1 + \theta(x_1) + \theta^2(x_1) + \cdots = -c_1\,;$$

si on les ajoute, les coefficients des racines autres que x_1 sont nuls dans la somme des premiers membres, et l'on obtient la valeur de x_1 ; si l'on multiplie de même les équations respectivement par $\omega^{-\alpha}$, $\omega^{-2\alpha}$, ..., on obtient la valeur de $\theta^\alpha(x_1)$, d'où les valeurs suivantes des racines :

$$(8)\quad \left\{\begin{aligned} x_1 &= \frac{1}{m}\left[-c_1+\sqrt[m]{T_1}+\frac{T_2}{T_1}(\sqrt[m]{T_1})^2+\ldots+\frac{T_{m-1}}{T_1}(\sqrt[m]{T_1})^{m-1}\right],\\ \theta(x_1) &= \frac{1}{m}\left[-c_1+\omega^{-1}\sqrt[m]{T_1}+\omega^{-2}\frac{T_2}{T_1}(\sqrt[m]{T_1})^2+\ldots\right.\\ &\qquad\left.+\,\omega^{-(m-1)}\frac{T_{m-1}}{T_1}(\sqrt[m]{T_1})^{m-1}\right],\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right.$$

On voit que les équations qui nous occupent sont résolubles par radicaux lorsqu'on adjoint au domaine de rationalité les racines m^{es} de l'unité, et qu'il suffit d'extraire la racine m^e d'une quantité connue rationnellement.

79. Lorsque les coefficients de $f(x)$ et de $\theta(x)$ sont des quantités réelles, le calcul numérique de $\sqrt[m]{T_1}$ peut être remplacé par le suivant :

La fonction

$$T_1 = [x_1+\omega\theta(x_1)+\cdots+\omega^{m-1}\theta^{m-1}(x_1)]^m$$

est rationnellement exprimable au moyen des coefficients de $f(x)$, de ceux de $\theta(x)$ et de ω ; si on la met sous la forme $\rho(\cos\vartheta+i\sin\vartheta)$, la présence de i tient à la racine ω, et le changement de ω en ω^{-1} a pour effet de changer i en $-i$; il transforme de plus T_1 en T_{m-1}, de sorte que l'on a

$$T_{m-1} = [x_1+\omega^{-1}\theta(x_1)+\omega^{-2}\theta^2(x_1)+\cdots]^m = \rho(\cos\vartheta-i\sin\vartheta),$$

$$T_1T_{m-1} = \rho^2.$$

D'autre part la fonction $\psi_1\psi_{m-1}$ est rationnellement exprimable au moyen des coefficients, car elle est de la forme $\psi_\alpha\psi_1^{m-\alpha}$ pour $\alpha = m-1$; de plus elle ne change pas de valeur quand on remplace ω par sa valeur conjuguée ω^{-1}, par conséquent elle est réelle ; si l'on représente par εU cette quantité, où U est positif et $\varepsilon = \pm 1$, on a, d'après la relation $T_1T_{m-1} = \psi_1^m\psi_{m-1}^m$, l'égalité

$$\rho^2 = \varepsilon^m U^m ;$$

il faut que ε^m soit égal à l'unité, puisque U est positif ; on conclut de là, en prenant la racine $2m^e$ arithmétique des deux membres,

$$\sqrt[m]{\rho} = \sqrt[2]{U},$$

et la racine m^e de T_1, qui est celle de $\rho(\cos\vartheta+i\sin\vartheta)$, a pour

valeur

$$\sqrt[m]{T_1} = \sqrt[2]{U}\left(\cos\frac{\vartheta + 2k\pi}{m} + i \sin\frac{\vartheta + 2k\pi}{m}\right).$$

Dans ce cas, la résolution de l'équation exige : 1° l'extraction de la racine carrée d'une quantité U que l'on peut calculer rationnellement ; 2° la division en m parties égales d'un angle que l'on peut construire.

80. Considérons une équation $f(x) = 0$ irréductible, de degré premier, et telle qu'une racine x'_1 soit une fonction rationnelle d'une autre racine x_1 ; d'après ce que nous avons vu au début de ce chapitre, les racines doivent se partager en ν séries d'un même nombre m d'éléments ; le produit νm ne peut être premier que si $\nu = 1$, car m est au moins égal à deux ; les racines forment alors une seule série de la forme

$$x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots,\ \theta^{m-1}(x_1),$$

et l'équation est résoluble algébriquement. On peut donc énoncer le théorème suivant :

Théorème. — *Si une équation irréductible de degré premier possède la propriété qu'une racine soit une fonction rationnelle d'une autre, elle est résoluble algébriquement.*

81. Revenons à l'équation de degré m dont les racines sont données par les formules (8) ; elles conviennent à tous les cas, mais lorsque m est un nombre composé, l'extraction des radicaux d'indice m se ramène, comme on le sait, à celle de radicaux successifs d'indices premiers; nous allons voir comment on peut, dans ce cas, simplifier la méthode précédente au point de vue du calcul numérique des racines.

Soit $m = m_1 n_1$; remplaçons dans ψ_1 ω par une racine primitive ω_1 de l'équation $x^{m_1} - 1 = 0$; nous aurons

$$\begin{aligned}\psi_1 = {} & x_1 + \theta^{m_1}(x_1) + \theta^{2m_1}(x_1) + \cdots + \theta^{(n_1-1)m_1}(x_1) \\ & + \omega_1[\theta(x_1) + \theta^{m_1+1}(x_1) + \cdots + \theta^{(n_1-1)m_1+1}(x_1)] \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & + \omega_1^{m_1-1}[\theta^{m_1-1}(x_1) + \theta^{2m_1-1}(x_1) + \cdots + \theta^{n_1 m_1-1}(x_1)],\end{aligned}$$

ce que nous écrirons

$$\psi_1 = \chi_0 + \omega_1\chi_1 + \cdots + \omega_1^{m_1-1}\chi_{m_1-1}.$$

La fonction

$$T_1 = \psi_1^{m_1} = (\chi_0 + \omega_1\chi_1 + \cdots + \omega_1^{m_1-1}\chi_{m_1-1})^{m_1}$$

reste invariable par le changement de x_1 en $\theta(x_1)$, car il a pour effet de permuter circulairement les éléments $\chi_0, \chi_1, \ldots, \chi_{m_1-1}$; par suite cette fonction s'exprime rationnellement, et l'on a, en extrayant une racine d'indice m_1,

$$\psi_1 = \sqrt[m_1]{T_1}.$$

Par un raisonnement identique à celui que nous avons fait, les fonctions $\psi_2, \psi_3, \ldots, \psi_{m_1-1}$ obtenues en remplaçant ω_1 par les racines $\omega_1^2, \omega_1^3, \ldots, \omega_1^{m_1-1}$ sont telles que les expressions

$$\psi_\alpha \psi_1^{m_1-\alpha} = T_\alpha$$

soient des fonctions rationnelles des coefficients de l'équation, et l'on en déduit que les fonctions $\chi_0, \chi_1, \chi_2, \ldots, \chi_{m_1-1}$ sont données par la formule suivante, où α prend les valeurs $0, 1, 2, \ldots, m_1 - 1$,

$$(9) \quad \chi_\alpha = \frac{1}{m_1}\left[-c_1 + \omega_1^{-\alpha}\sqrt[m_1]{T_1} + \omega_1^{-2\alpha}\frac{T_2}{T_1}(\sqrt[m_1]{T_1})^2 + \cdots\right].$$

Lorsqu'on a déterminé une de ces quantités, par exemple χ_0, on peut déterminer rationnellement les fonctions symétriques des racines x_1, $\theta^{m_1}(x_1)$, $\theta^{2m_1}(x_1)$, $\ldots$, $\theta^{(n_1-1)m_1}(x_1)$, car ces fonctions symétriques appartiennent au même groupe de substitutions que χ_0; on peut alors calculer les coefficients de l'équation à laquelle satisfont ces racines; mais si l'on pose $\theta^{m_1} = \theta_1$, elles sont de la forme

$$x_1, \qquad \theta_1(x_1), \qquad \theta_1^2(x_1), \qquad \ldots, \qquad \theta_1^{(n_1-1)}(x_1),$$

et la méthode précédente est applicable à leur détermination.

Les autres séries de racines dont les sommes sont respectivement $\chi_1, \chi_2, \ldots, \chi_{m_1-1}$ sont déterminées de la même manière au moyen de chacune de ces quantités; il en résulte que les m racines de $f(x) = 0$ sont exprimées par des radicaux d'indices m_1 et n_1 et par des racines de l'unité satisfaisant aux équations

$$x^{m_1} - 1 = 0, \qquad x^{n_1} - 1 = 0.$$

Remarquons qu'il suffit de connaître une seule des m racines de la suite (7) pour calculer toutes les autres, car si x_1' est une quelconque d'entre elles, les autres sont égales à $\theta(x_1'), \theta^2(x_1'), \ldots, \theta^{m-1}(x_1')$, et sont des fonctions rationnelles de la première; on en conclut que l'équation sera résolue dès que l'on aura déterminé une des quantités χ et une des racines qui en dépendent.

On a donc le résultat suivant :

THÉORÈME. — *Si* $m = m_1 n_1$, *la résolution de l'équation* $f(x) = 0$, *de degré* m, *dont les racines sont celles de la suite* (7), *se ramène à celle de deux équations successives, de degrés* m_1 *et* n_1, *auxquelles est applicable la méthode exposée précédemment; les coefficients de la première étant des quantités connues, et ceux de la seconde des fonctions rationnelles d'une racine de la précédente.*

Si n_1 est lui-même un nombre composé égal à $m_2 n_2$, chaque équation de degré n_1 dont les coefficients dépendent de l'une des quantités χ peut elle-même être résolue au moyen de deux équations de degrés m_2 et n_2 comme nous venons de l'indiquer ; en continuant de cette façon, on obtient la conclusion suivante :

THÉORÈME. — *Pour résoudre une équation de degré*

$$m = m_1 m_2 \ldots m_p$$

jouissant de la propriété donnée, il suffit :

1° *de calculer une racine primitive de chacune des équations*

$$x^{m_1} - 1 = 0, \qquad x^{m_2} - 1 = 0, \qquad \ldots, \qquad x^{m_p} - 1 = 0;$$

2° *d'extraire des racines successives d'indices* $m_1, m_2, \ldots, m_p$ *de quantités s'exprimant chacune rationnellement au moyen des radicaux qui la précèdent, des coefficients de l'équation, et des racines des équations binomes dont on vient de parler.*

Les nombres $m_1, m_2, \ldots, m_p$ peuvent être égaux ou inégaux ; si donc ce sont les facteurs premiers du nombre m, on voit comment la résolution de l'équation de degré m se ramène à celles d'équations successives de degrés premiers. En particulier, si les nombres $m_1, m_2, \ldots, m_p$ sont égaux à 2, les racines de l'unité sont égales à ± 1, et les radicaux ont leur indice égal à 2 ; par suite on a le corollaire suivant :

COROLLAIRE. — *Toute équation de degré* 2^p *dont les racines sont représentées par*

$$x_1, \theta(x_1), \theta^2(x_1), \ldots, \theta^{2^p-1}(x_1)$$

est résoluble à l'aide de p *racines carrées successives.*

82. Pour donner un exemple d'une suite de racines analogue à la suite (7), cherchons si l'on peut prendre pour $\theta(x_1)$ une fraction

rationnelle de la forme

$$\theta(x) = \frac{ax+b}{cx+d},$$

où a, b, c, d sont réels ; il faut d'abord que $\delta = ad - bc$ soit $\neq 0$, car sinon $\theta(x)$ serait constant ; on peut alors, en multipliant a, b, c, d par un même nombre si c'est nécessaire, supposer δ égal à ± 1 ; soient x' et x'' les racines de l'équation $\theta(x) = x$, qui peut s'écrire

$$ax + b - x(cx+d) = x(a - cx) + b - dx = 0.$$

Supposons d'abord qu'elles soient distinctes, et formons l'expression

$$\frac{\theta(x) - x'}{\theta(x) - x''} = \frac{ax + b - x'(cx+d)}{ax + b - x''(cx+d)} = \frac{(a - cx')x + b - dx'}{(a - cx'')x + b - dx''};$$

d'après l'équation à laquelle satisfont x' et x'', elle s'écrit encore

$$\frac{\theta(x) - x'}{\theta(x) - x''} = \frac{a - cx'}{a - cx''} \cdot \frac{x - x'}{x - x''} = \mathrm{M}\,\frac{x - x'}{x - x''},$$

où le facteur M peut être mis sous l'une des formes suivantes, en utilisant la remarque que $\delta = \pm 1$,

$$\mathrm{M} = \frac{(a - cx')^2}{\delta} = \delta\left[\frac{a+d}{2} - \sqrt{\left(\frac{a+d}{2}\right)^2 - \delta}\,\right]^2.$$

Comme on obtient, en remplaçant x par $\theta(x)$,

$$\frac{\theta^2(x) - x'}{\theta^2(x) - x''} = \mathrm{M}\,\frac{\theta(x) - x'}{\theta(x) - x''} = \mathrm{M}^2\,\frac{x - x'}{x - x''},$$

on aura en général

$$\frac{\theta^m(x) - x'}{\theta^m(x) - x''} = \mathrm{M}^m\,\frac{x - x'}{x - x''}.$$

Pour que $\theta^m(x) = x$, il faut et il suffit que $\mathrm{M}^m = 1$, ce qui donne

$$\delta^m\left[\frac{a+d}{2} - \sqrt{\left(\frac{a+d}{2}\right)^2 - \delta}\,\right]^{2m} = 1.$$

Si les racines x' et x'' sont imaginaires, il faut que $\delta = +1$, car sinon le radical serait réel ; on doit de plus avoir

$$\frac{a+d}{2} - \sqrt{\left(\frac{a+d}{2}\right)^2 - 1} = \cos\frac{k\pi}{m} + i\sin\frac{k\pi}{m};$$

il suffit de poser, pour satisfaire à cette condition,

$$(10) \qquad a + d = 2 \cos \frac{k\pi}{m},$$

k étant premier avec m si m est le premier nombre pour lequel $\theta^m(x) = x$. Si les racines x' et x'' sont réelles, il faut, dans le cas où $\delta = +1$, que

$$\frac{a+d}{2} - \sqrt{\left(\frac{a+d}{2}\right)^2 - 1} = \pm 1,$$

ce qui donne $a + d = \pm 2$, d'où $x' = x''$, contrairement à l'hypothèse ; dans le cas où $\delta = -1$, il faut que m soit pair et que $a + d = 0$, ce qui donne $M^2 = 1$; ce cas ne peut exister que si $m = 2$, et le résultat est fourni par l'équation (10) lorsqu'on y fait $m = 2$.

Nous supposons maintenant $x' = x''$, ce qui exige $\delta = 1$ et $a + d = \pm 2$. On vérifie que l'on a alors

$$\frac{1}{\theta(x) - x'} - \frac{1}{x - x'} = \frac{2c}{a+d},$$

de sorte que, en appelant N la valeur du second membre, remplaçant x par $\theta(x)$ et répétant cette opération, il vient

$$\frac{1}{\theta^m(x) - x'} = \frac{1}{x - x'} + m\mathrm{N}.$$

Pour que $\theta^m(x) = x$, il faut que $\mathrm{N} = 0$, alors on a $\theta(x) = x$, ce qui est impossible.

Il n'y a donc que les conditions

$$a + d = 2 \cos \frac{k\pi}{m}, \qquad ad - bc = 1$$

qui soient nécessaires et suffisantes pour que la fonction $\theta(x)$ réponde à la question.

Comme application, considérons l'équation donnant $\operatorname{tg} \frac{\varphi}{m}$ connaissant $\operatorname{tg} \varphi$; si nous posons $\operatorname{tg} \varphi = a$, et $\operatorname{tg} \frac{\varphi}{m} = x$, cette équation est

$$a = \frac{1}{i} \cdot \frac{(1 + ix)^m - (1 - ix)^m}{(1 + ix)^m + (1 - ix)^m},$$

et est de degré m, à coefficients réels. Ses racines sont

$$\operatorname{tg}\frac{\varphi}{m},\quad \operatorname{tg}\left(\frac{\varphi}{m}+\frac{\pi}{m}\right),\quad \operatorname{tg}\left(\frac{\varphi}{m}+\frac{2\pi}{m}\right),\ \ldots,\quad \operatorname{tg}\left(\frac{\varphi}{m}+\frac{(m-1)\pi}{m}\right),$$

et sont toutes des fonctions rationnelles de l'une d'entre elles ; en désignant l'une de ces racines par x_1, et posant

$$\theta(x) = \frac{x + \operatorname{tg}\frac{\pi}{m}}{1 - x\operatorname{tg}\frac{\pi}{m}},$$

les autres sont égales à $\theta(x_1)$, $\theta^2(x_1)$, ..., $\theta^{m-1}(x_1)$.

En écrivant la fonction rationnelle précédente sous la forme

$$\theta(x) = \frac{x\cos\frac{\pi}{m} + \sin\frac{\pi}{m}}{-x\sin\frac{\pi}{m} + \cos\frac{\pi}{m}},$$

on vérifie bien qu'elle satisfait aux conditions que nous avons trouvées précédemment. On conclut de là que l'équation dont dépend $\operatorname{tg}\frac{\varphi}{m}$ est résoluble par radicaux lorsqu'on adjoint au domaine de rationalité, constitué par a et par les nombres entiers, les racines m^{es} de l'unité et les quantités $\cos\frac{\pi}{m}$ et $\sin\frac{\pi}{m}$.

83. Nous allons maintenant considérer les équations déjà étudiées par Abel et appelées par Kronecker et M. Jordan équations abéliennes.

Une équation irréductible ou non est dite abélienne si toutes ses racines sont des fonctions rationnelles de l'une d'entre elles x_1 et si

$$x_\alpha = \theta_\alpha(x_1), \qquad x_\beta = \theta_\beta(x_1)$$

étant deux racines quelconques exprimées au moyen de x_1, les fonctions θ_α et θ_β jouissent de la propriété d'être échangeables, c'est-à-dire sont telles que l'on ait

$$\theta_\alpha\theta_\beta(x_1) = \theta_\beta\theta_\alpha(x_1).$$

Les équations que nous avons étudiées, pour lesquelles les racines s'expriment toutes sous la forme (7)

$$x_1, \qquad \theta(x_1), \qquad \theta^2(x_1), \qquad \ldots, \qquad \theta^{m-1}(x_1),$$

sont des équations abéliennes ; nous dirons qu'elles sont simples ;

nous avons vu qu'elles sont résolubles par radicaux, lorsqu'on adjoint au domaine de rationalité les racines de l'unité ; nous verrons qu'il en est de même des équations abéliennes générales, comme l'a démontré Abel (*).

Nous allons ramener d'abord la résolution des équations générales à celles d'équations irréductibles jouissant de la même propriété en démontrant le théorème suivant :

THÉORÈME. — *Tout facteur irréductible du premier membre d'une équation abélienne, égalé à zéro, donne de nouveau une équation abélienne.*

Soit $f(x) = f_1(x)f_2(x)\ldots$ le premier membre de l'équation donnée décomposé en ses facteurs irréductibles, $f_1(x)$ étant celui qui contient la racine x_1 ; il est évident que l'équation $f_1(x) = 0$ est abélienne, car ses racines s'expriment rationnellement au moyen de x_1, et les fonctions qui les représentent sont échangeables ; désignons-les par x_1, $\theta_1(x_1)$, ..., $\theta_{m-1}(x_1)$. Soit maintenant $f_2(x)$ un autre facteur contenant une racine que nous appellerons $\vartheta(x_1)$; les équations

$$f_1(x) = 0, \qquad f_2[\vartheta(x)] = 0$$

ont en commun la racine x_1 ; par suite la seconde admet les m racines de la première et $f_2(x)$ est satisfaite par les valeurs

$$\vartheta(x_1),\ \vartheta\theta_1(x_1),\ \ldots,\ \vartheta\theta_{m-1}(x_1),$$

qu'on peut écrire, d'après la propriété des fonctions θ et en posant $\vartheta(x_1) = x_2$:

$$x_2,\ \theta_1(x_2),\ \ldots,\ \theta_{m-1}(x_2).$$

Le produit

$$[x - x_2][x - \theta_1(x_2)]\ldots[x - \theta_{m-1}(x_2)]$$
$$= [x - \vartheta(x_1)][x - \vartheta\theta_1(x_1)]\ldots[x - \vartheta\theta_{m-1}(x_1)]$$

étant symétrique par rapport aux racines de $f_1(x)$, est rationnel, et constitue un diviseur rationnel du polynome $f_2(x)$; comme ce dernier est irréductible, on voit que l'équation $f_2(x) = 0$ ne peut avoir d'autres racines que les m quantités précédentes ; leurs propriétés montrent que cette équation est abélienne.

La même démonstration s'applique aux équations obtenues en

(*) ABEL, *Œuvres complètes*, t. I, nº XI, p. 114-140.

annulant les autres facteurs irréductibles de $f(x)$; elle nous indique de plus que tous ces facteurs ont le même degré.

84. Nous nous limiterons par suite aux équations abéliennes irréductibles, et nous emploierons à leur égard la méthode indiquée par Kronecker (*).

Soit $f(x) = 0$ une telle équation de degré n, x_1 une racine au moyen de laquelle s'expriment toutes les autres, et $\theta_1(x_1)$ une autre racine ; d'après la propriété de l'équation donnée d'être irréductible, les expressions

$$x_1,\ \theta_1(x_1),\ \theta_1^2(x_1),\ \ldots,\ \theta_1^{\nu_1-1}(x_1),\ \ldots$$

sont encore des racines; comme le nombre de leurs valeurs distinctes est au plus égal à n, il existe, ainsi qu'on l'a vu au § 76, un exposant ν_1 pour lequel $\theta_1^{\nu_1}(x_1) = x_1$, les ν_1 racines $x_1, \theta_1(x_1), \ldots, \theta_1^{\nu_1-1}(x_1)$ étant distinctes. Si $\nu_1 = n$, $f(x) = 0$ est une équation abélienne simple, comme celle que nous avons considérée au § 78 ; si au contraire ν_1 est inférieur à n, on peut trouver une deuxième fonction $\theta_2(x_1)$ représentant une nouvelle racine, et un exposant ν_2 analogue à ν_1 tel que $\theta_2^{\nu_2}(x_1) = x_1$, et ainsi de suite jusqu'à une fonction $\theta_\lambda(x_1)$ et un exposant ν_λ tel que $\theta_\lambda^{\nu_\lambda}(x_1) = x_1$.

Il peut arriver que les racines ainsi formées ne soient pas toutes distinctes et soient en nombre supérieur à n. Supposons que l'une des fonctions que nous venons de choisir, telle que $\theta_\alpha(x_1)$ constitue une racine non encore obtenue; $\theta_\alpha(x_1), \theta_\alpha^2(x_1), \ldots, \theta_\alpha^{\nu_\alpha-1}(x_1)$ sont bien des racines distinctes les unes des autres, mais l'une d'elles peut être égale à l'une des racines autres que x_1 formées précédemment ; ou bien encore θ_α peut être une combinaison de plusieurs fonctions $\theta_\beta, \theta_\gamma, \ldots$ de la suite $\theta_1, \theta_2, \ldots, \theta_{\alpha-1}$, et avoir la même valeur que $\theta_\beta^h \theta_\gamma^k \ldots$ Nous allons réduire les expressions θ au nombre minimum d'éléments (**).

Nous dirons qu'une fonction θ_α appartient à l'exposant ν_α si ce nombre est le plus petit pour lequel on ait $\theta_\alpha^{\nu_\alpha}(x_1) = x_1$; tous les autres jouissant de la même propriété sont des multiples de ν_α. Si d est un diviseur de ν_α, $\theta_\alpha^{\frac{\nu_\alpha}{d}}$ appartient à l'exposant d ; on voit de

(*) Kronecker « Ueber abelsche Gleichungen », *Monatsberichte*, 1877, p. 845.

(**) Comparer Kronecker « Auseinandersetzung einigen Eigenschaften der Klassenzahl idealer Zahlen », *Monatsberichte*, 1870, p. 881, et Netto, *Substitutionentheorie*, p. 144.

plus que si deux fonctions θ', θ'' appartiennent à des exposants ν', ν'' premiers entre eux, la fonction $\theta'\theta''(x_1)$ appartient à $\nu'\nu''$. En effet, soit h un nombre tel que l'on ait $(\theta'\theta'')^h(x_1) = x_1$; l'égalité précédente subsistera si l'on élève le premier membre à la puissance symbolique ν'; comme on a $(\theta'\theta'')^{h\nu'} = \theta'^{h\nu'}\theta''^{h\nu'}$ et que $\theta''^{h\nu'}(x_1) = x_1$, il faut que $h\nu'$ soit un multiple de ν''; on voit de même que $h\nu''$ doit être un multiple de ν', et la plus petite valeur que l'on puisse donner à h est le produit $\nu'\nu''$.

Plus généralement, considérons deux fonctions θ' et θ'' dont les exposants ν' et ν'' ont un plus grand commun diviseur d; posons $\nu' = d\nu'_1$ et $\nu'' = d\nu''_1$, ν'_1 et ν''_1 étant premiers entre eux, et désignons par m le plus petit commun multiple $d\nu'_1\nu''_1$ de ν' et ν''. Toute combinaison de θ' et θ'', telle que $\theta'^h\theta''^k$ appartient à un exposant égal à m ou à l'un de ses sous-multiples; mais on peut toujours en former une appartenant au nombre m lui-même; décomposons en effet le plus grand commun diviseur d en deux facteurs d' et d'' premiers entre eux et respectivement premiers avec ν'_1 et ν''_1; les deux nombres $\frac{\nu'}{d'} = \frac{d\nu'_1}{d'} = d''\nu'_1$ et $\frac{\nu''}{d''} = \frac{d\nu''_1}{d''} = d'\nu''_1$ sont premiers entre eux et ont pour produit m; dès lors, d'après ce que nous avons vu, le produit symbolique des deux fonctions $\theta'^{d'}$ et $\theta''^{d''}$ d'exposants respectifs $\frac{\nu'}{d'}$ et $\frac{\nu''}{d''}$ appartient au nombre m.

On conclut de là que si n_1 est le plus petit commun multiple de $\nu_1, \nu_2, \ldots, \nu_\lambda$, on pourra former au moyen de $\theta_1, \theta_2, \ldots, \theta_\lambda$ une fonction appartenant à n_1; nous la désignerons par ϑ_1; toutes les combinaisons des fonctions θ appartiennent à un nombre égal à n_1 ou à l'un de ses diviseurs. Reprenons le système $\theta_1, \theta_2, \ldots, \theta_\lambda$ et excluons-en toute fonction θ_β égale au produit d'une de celles qui la précèdent dans la suite et d'une puissance de ϑ_1, c'est-à-dire satisfaisant à une égalité de la forme

$$\theta_\beta(x_1) = \theta_\alpha\vartheta_1^k(x_1) \qquad (\alpha < \beta \quad \text{ou} \quad = 0);$$

il restera un système $\theta'_1, \theta'_2, \ldots, \theta'_\mu$ composé d'une partie des fonctions du système primitif; nous dirons qu'elles appartiennent relativement à ϑ_1 aux exposants respectifs $\nu'_1, \nu'_2, \ldots, \nu'_\mu$ si ces nombres sont les plus petits pour lesquels on ait des égalités telles que

$$\theta_1'^{\nu'_1}(x_1) = \vartheta_1^{k_1}(x_1), \qquad \theta_2'^{\nu'_2}(x_1) = \vartheta_1^{k_2}(x_1), \qquad \ldots;$$

par un raisonnement analogue au précédent, on pourra former une fonction ϑ'_2 telle que, n_2 étant le plus petit commun multiple de $\nu'_1, \nu'_2, \ldots, \nu'_\mu$, la puissance $\vartheta'^{n_2}_2$ soit la première se réduisant à une puissance de ϑ_1 ; on aura par exemple

$$\vartheta'^{n_2}_2(x_1) = \vartheta^k_1(x_1) ;$$

toute fonction θ' appartiendra, relativement à ϑ_1, à un exposant égal à n_2 ou à un sous-multiple de ce nombre.

n_2 est lui-même, d'après ce qu'on a vu, un diviseur de n_1; si $n_1 = n_2 d$, on aura

$$x_1 = \vartheta'^{n_2 d}_2(x_1) = \vartheta^{kd}_1(x_1),$$

et comme l'exposant kd de ϑ_1, c'est-à-dire $k\dfrac{n_1}{n_2}$ doit être un multiple de n_1, il faut que k soit un multiple de n_2 tel que ρn_2, $(\rho > 1)$; il est alors permis de remplacer la fonction ϑ'_2 par

$$\vartheta_2 = \vartheta'_2 \vartheta'^{n_1 - \rho}_1,$$

qui appartient, non seulement par rapport à ϑ_1, mais encore par rapport à x_1, à l'exposant n_2 d'après l'égalité

$$\vartheta^{n_2}_2(x_1) = \vartheta'^{n_2}_2 \vartheta^{(n_1-\rho)n_2}_1(x_1) = \vartheta^{n_1 n_2}_1(x_1) = x_1,$$

et n_2 est le plus petit nombre jouissant de cette propriété.

De la même manière, on pourra exclure du système $\theta'_1, \theta'_2, \ldots, \theta'_\mu$ les fonctions pour lesquelles on ait une égalité telle que

$$\theta'_\beta(x_1) = \theta'_\alpha \vartheta^k_1 \vartheta^l_2(x_1) \qquad (\alpha < \beta \quad \text{ou} \quad = 0)$$

et continuer de cette façon ; finalement toutes les fonctions θ et leurs combinaisons pourront se mettre sous la forme

$$\vartheta^{h_1}_1 \vartheta^{h_2}_2 \ldots \vartheta^{h_\nu}_\nu(x_1) \qquad \left(\begin{array}{l} h_1 = 0, 1, 2, \ldots, n_1 - 1 \\ h_2 = 0, 1, 2, \ldots, n_2 - 1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ h_\nu = 0, 1, 2, \ldots, n_\nu - 1 \end{array}\right)$$

où les fonctions ϑ appartiennent respectivement aux exposants $n_1, n_2, \ldots, n_\nu$, relativement à celles d'indice moindre et aussi relativement à x_1, et où chacun des nombres $n_1, n_2, \ldots, n_\nu$ est divisible par le suivant.

Toutes les fonctions ainsi formées sont du reste distinctes, et représentent une fois et une seule toutes les racines, de sorte que le nombre de ces dernières est

$$n = n_1 n_2 \ldots n_\nu.$$

Nous supposerons donc que l'on ait exprimé toutes les racines

d'une équation abélienne irréductible sous la forme précédente au moyen de x_1, et nous remplacerons les lettres ϑ par θ dans ce qui suit.

85. Théorème. — *La condition nécessaire et suffisante pour qu'une équation irréductible soit abélienne est qu'on puisse attribuer aux racines des indices tels qu'une fonction cyclique de ces racines, à une ou plusieurs entrées, fasse partie du domaine de rationalité.*

La condition est nécessaire; supposons en effet qu'une équation soit abélienne, et qu'on ait exprimé les racines en fonction de l'une d'elles comme nous l'avons dit; affectons chacune d'elles de ν indices et posons

$$x_1 = x_{00\ldots 0},$$

$$\theta_1^{h_1}\theta_2^{h_2}\ldots\theta_\nu^{h_\nu}(x_1) = x_{h_1 h_2\ldots h_\nu};$$

toute fonction cyclique à ν entrées de ces racines, appartenant au groupe suivant (§ 30) :

$$\begin{array}{ll} | z_1 \quad z_1+1 | & (\text{mod. } n_1) \\ | z_2 \quad z_2+1 | & (\text{mod. } n_2) \\ \ldots\ldots\ldots\ldots & \\ | z_\nu \quad z_\nu+1 | & (\text{mod. } n_\nu) \end{array}$$

est rationnellement exprimable. Elle est en effet une fonction rationnelle de x_1; si nous la désignons par $C(x_1)$ et si nous remplaçons x_1 par une autre des racines de l'équation donnée, nous obtenons la même valeur qu'en effectuant sur la fonction cyclique C une des substitutions du groupe précédent; comme elles la laissent invariable, on a, en appelant pour un instant $x_1, x_2, \ldots, x_n$ les n racines,

$$C(x_1) = C(x_2) = \cdots = C(x_n),$$

d'où

$$C(x_1) = \frac{1}{n}[C(x_1) + C(x_2) + \cdots + C(x_n)];$$

le second membre étant une fonction symétrique, on voit que la fonction cyclique considérée s'exprime rationnellement au moyen des coefficients de l'équation.

Réciproquement, si une fonction cyclique des racines fait partie du domaine de rationalité, l'équation est abélienne.

Nous avons vu en effet au § 31 que les quantités $x_{h_1 h_2\ldots h_\nu}$ s'expriment rationnellement au moyen de l'une d'elles $x_{00\ldots 0}$, et d'une

fonction cyclique particulière quelconque ; si celle-ci fait partie du domaine de rationalité, chaque racine est une fonction rationnelle de $x_{00\ldots 0}$, et les fonctions θ qui les expriment sont échangeables, par suite l'équation est abélienne.

Nous dirons qu'une telle équation, dont le groupe est un groupe cyclique à ν entrées, est une équation abélienne de rang ν.

86. Nous allons ramener la résolution des équations abéliennes générales à celle des équations simples à l'aide des considérations suivantes.

Parmi les $n = n_1 n_2 \ldots n_\nu$ racines $x_{h_1 h_2 \ldots h_\nu}$, considérons celles pour lesquelles μ des indices, par exemple $h_1, h_2, \ldots, h_\mu$, ont des valeurs fixes $\alpha_1, \alpha_2, \ldots, \alpha_\mu$, et les autres variables ; leur nombre est $n_{\mu+1}\, n_{\mu+2} \ldots n_\nu$. Prenons une fonction cyclique de ces racines, relativement au groupe déterminé par

$$| z_{\mu+1} \quad z_{\mu+1} + 1 |, \quad | z_{\mu+2} \quad z_{\mu+2} + 1 |, \quad \ldots, \quad | z_\nu \quad z_\nu + 1 | ;$$

si nous la représentons par $y_{\alpha_1 \alpha_2 \ldots \alpha_\mu}$, elle a pour toutes les substitutions du groupe cyclique $n_1 n_2 \ldots n_\mu$ valeurs distinctes, obtenues en faisant varier les indices α ; je dis que ce sont les racines d'une équation abélienne ; en effet, toute fonction cyclique des y reste invariable pour les substitutions cycliques effectuées sur les racines x, et est rationnellement exprimable, par suite l'équation est abélienne d'après le théorème précédent.

Lorsqu'on a résolu l'équation abélienne de rang μ et de degré $n_1 n_2 \ldots n_\mu$ donnant les valeurs des fonctions y, on peut déterminer au moyen de $y_{\alpha_1 \alpha_2 \ldots \alpha_\mu}$ les coefficients de l'équation satisfaite par les racines $x_{\alpha_1 \alpha_2 \ldots \alpha_\mu h_{\mu+1} \ldots h_\nu}$ lorsqu'on fait varier les derniers indices ; cette équation est abélienne quand on adjoint au domaine de rationalité la quantité $y_{\alpha_1 \alpha_2 \ldots \alpha_\mu}$, car les fonctions cycliques des racines font partie du nouveau domaine. Si l'on prend $\mu = 1$, les fonctions y sont racines d'une équation abélienne simple de degré n_1 résoluble par radicaux, ainsi que nous l'avons vu ; lorsqu'on a calculé ses racines, la résolution de l'équation donnée se ramène à celle de n_1 équations abéliennes de rang $\nu - 1$ et de degré $n_2 n_3 \ldots n_\nu$, auxquelles est applicable la même méthode. Si l'on remarque que la connaissance d'une seule racine d'une équation abélienne entraîne celle de toutes les autres, on peut énoncer le théorème et le corollaire suivants :

Théorème. — *L'équation abélienne générale de rang* ν *et de degré* $n = n_1 n_2 \ldots n_\nu$ *se résout au moyen de* ν *équations abéliennes simples successives, de degrés* $n_1, n_2, \ldots, n_\nu$ (*).

Corollaire I. — *Toute équation abélienne est résoluble par radicaux lorsqu'on adjoint au domaine de rationalité les racines de l'unité.*

Pratiquement, on formera les fonctions symétriques

$$y_{\alpha_1} = \Sigma_{h_2 h_3 \cdots h_\nu} x_{\alpha_1 h_2 \cdots h_\nu} \qquad (\alpha_1 = 0, 1, \ldots, n_1 - 1)$$

et la résolvante

$$T_1 = [y_0 + \omega_1 y_1 + \omega_1^2 y_2 + \cdots + \omega_1^{n_1 - 1} y_{n_1 - 1}]^{n_1},$$

où ω_1 est une racine primitive de $x^{n_1} - 1 = 0$; elle est rationnellement exprimable et, au moyen de $\sqrt[n_1]{T_1}$ et de ω_1 on détermine $y_0, y_1, y_2, \ldots, y_{n_1 - 1}$; les fonctions cycliques des racines x qui composent y_{α_1} sont connues au moyen de cette quantité, et l'on continue de proche en proche.

Si l'on remarque qu'une équation abélienne simple de degré composé se résout au moyen d'une suite d'équations de même nature et de degré premier (§ 81), on peut énoncer ce deuxième corollaire :

Corollaire II. — *Toute équation abélienne se résout au moyen d'équations abéliennes simples successives de degré premier.*

87. Nous terminerons ce chapitre par un exposé succinct des recherches de Kronecker sur la nature des racines des équations abéliennes, et leur expression générale au moyen des racines de l'unité; elles ont été exposées par lui dans différents articles insérés dans les *Monatsberichte* (1853, 1856 et 1877), et une partie en a été reproduite dans l'*Algèbre supérieure,* de Serret (t. II, p. 693).

D'après ce qui précède, il suffit de nous limiter au cas d'une équation abélienne irréductible et simple, de plus de degré premier, car c'est à la résolution d'une suite d'équations de cette forme que se ramène celle des équations générales.

Soient $x_0, x_1, \ldots, x_{n-1}$ les racines d'une équation de degré premier n; leur détermination dépend du calcul des fonctions cycliques

---

(*) Kronecker, *Monatsberichte*, 1877, p. 847; Netto, *Substitutionentheorie*, p. 208. Consulter aussi Jordan, *Traité des Substitutions,* §§ 405-407.

résolvantes rationnellement exprimables, de la forme

$$w_k = \psi_k^n = \left[\sum_{r=0}^{n-1} \omega^{kr} x_r\right]^n \qquad (\omega^n = 1);$$

on a en effet

(11) $$n x_h = \Sigma_k \omega^{-hk} \psi_k.$$

Si l'on remplace ω par ω^t, on remarque que la fonction

$$\psi_{ht}^l \cdot \psi_{h't}^{l'} \cdots$$

est rationnellement exprimable au moyen des coefficients de l'équation et de ω^t dès que $lh + l'h' + \ldots$ est $\equiv 0 \pmod{n}$; on en déduit en particulier, φ_h désignant une fonction rationnelle,

$$\frac{\psi_{ht}}{\psi_t^h} = \varphi_h(\omega^t); \qquad \frac{\psi_h}{\psi_1^h} = \varphi_h(\omega).$$

Si l'on pose $\psi_t^n = f(\omega^t)$ et $\psi_1^n = f(\omega)$, on en tire

$$\psi_h = \varphi_h(\omega) f(\omega)^{\frac{h}{n}}.$$

Prenons pour h une racine primitive du nombre n, telle que, si $h^{n-1} = 1 + n\rho$, le nombre ρ ne soit pas divisible par n, et considérons le produit

(12) $$\left(\frac{\psi_{ht}}{\psi_t^h}\right)^{h^{n-2}} \left(\frac{\psi_{h^2t}}{\psi_{ht}^h}\right)^{h^{n-3}} \cdots \left(\frac{\psi_{h^{n-1}t}}{\psi_{h^{n-2}t}^h}\right) = \varphi_h(\omega^t)^{h^{n-2}} \varphi_h(\omega^{ht})^{h^{n-3}} \cdots \varphi_h(\omega^{h^{n-2}t}).$$

Le premier membre se réduit à $\psi_t^{1-h^{n-1}} = \psi_t^{-n\rho}$; si l'on prend σ tel que

$$\rho + \sigma \equiv 0 \pmod{n},$$

σ n'est pas nul par hypothèse; le produit $\psi_t^\rho \psi_t^\sigma$ est rationnellement exprimable, et l'on a par exemple

$$\psi_t^\rho \psi_t^\sigma = \chi(\omega^t),$$

d'où

$$\psi_{t\sigma} = \psi_t^\sigma \varphi_\sigma(\omega^t) = \psi_t^{-\rho} \varphi_\sigma(\omega^t) \chi(\omega^t).$$

On peut poser $t\sigma \equiv k$ et exprimer ω^t en fonction de ω^k, qui est aussi racine primitive; en désignant $\varphi_\sigma(\omega^t)\chi(\omega^t)$ par $F(\omega^k)$ et remplaçant $\psi_t^{-\rho}$ par la puissance $\frac{1}{n}$ du deuxième membre de l'équa-

tion (12), on arrive pour déterminer $\psi_{t\sigma} = \psi_k$ à la formule

$$\psi_k = F(\omega^k)\left[\prod_{\lambda=1}^{n-1} \varphi_h(\omega^{h^{\lambda-1}t})^{h^{n-\lambda-1}}\right]^{\frac{1}{n}}.$$

Il reste à simplifier la parenthèse ; si l est le nombre tel que $l\sigma \equiv 1 \pmod{n}$, on a

$$t\sigma l \equiv kl, \qquad t \equiv kl;$$

on peut remplacer ω^l par sa valeur en fonction de ω^h et poser

$$\varphi_h(\omega^l) = f_1(\omega^h);$$

alors

$$\varphi_h(\omega^{h^{\lambda-1}t})^{h^{n-\lambda-1}} = \varphi_h(\omega^{h^{\lambda-1}kl})^{h^{n-\lambda-1}} = f_1(\omega^{h^\lambda k})^{h^{n-\lambda-1}} = f_1(\omega^{\alpha k})^\beta,$$

α prenant avec le reste de h^λ toutes les valeurs $1, 2, \ldots, n-1$ quand λ varie, et β satisfaisant à la condition $\alpha\beta \equiv 1 \pmod{n}$; en modifiant la fonction $F(\omega^k)$, on peut prendre β entre 0 et $n-1$.

On peut enfin poser $\alpha k \equiv r$, de sorte que $\beta r \equiv k$, et si l'on choisit s de façon que $rs \equiv 1 \pmod{n}$, β sera déterminé par la congruence $\beta \equiv ks$; on aura donc la formule

$$(13) \qquad \psi_k = F(\omega^k)\prod_{r=1}^{n-1} f_1(\omega^r)^{\frac{(sk)}{n}},$$

où r varie de 1 à $n-1$, s est donné par $rs \equiv 1 \pmod{n}$, et sk doit être réduit à son reste (mod. n).

Telle est la formule donnée par Kronecker et déjà trouvée par Kummer (*Journal de Crelle*, t. 35, p. 363) ; F et f_1 désignent des fonctions rationnelles, et la formule (11) fournit la valeur des racines $x_0, x_1, \ldots, x_{n-1}$.

88. Il reste à démontrer la réciproque ; quelles que soient les fonctions F et f_1 rationnelles dans le domaine donné, les formules (11) et (13) donnent les racines d'une équation abélienne.

Remarquons d'abord que ψ_k^n est une fonction rationnelle de ω ; on a en outre

$$\frac{\psi_{ht}}{\psi_t^h} = F(\omega^{ht})F(\omega^t)^{-h}\Pi_r f_1(\omega^r)^{\frac{(sht)}{n} - \frac{h(st)}{n}};$$

l'exposant de f_1 étant entier et ω^r étant une fonction de ω^t, on voit

que le second membre est une fonction rationnelle de ω^t ; nous pourrons donc poser, en le désignant par $\varphi_h(\omega^t)$,

$$\psi_{ht} = \psi_t^h \varphi_h(\omega^t). \tag{14}$$

Nous allons montrer que les fonctions symétriques des racines ainsi que les fonctions cycliques sont rationnelles ; il suffit de le faire voir en particulier pour Σx_h^λ et $\Sigma x_{h+1} x_h^\lambda$; nous partirons pour cela de la formule (11) où l'on peut remplacer k par kt si t est premier avec n ; on a ainsi

$$nx_h = \Sigma_k \omega^{-hkt} \psi_{kt},$$

$$x_h^\lambda = \text{A}\Sigma_{k_1 k_2 \ldots} \omega^{-h(k_1+k_2+\ldots)t} \psi_{k_1 t} \psi_{k_2 t} \ldots,$$

où A est un coefficient numérique, et

$$\Sigma_h x_h^\lambda = \text{A}\Sigma_{k_1 k_2 \ldots} \psi_{k_1 t} \psi_{k_2 t} \ldots (\Sigma_h \omega^{-h(k_1+k_2+\ldots)t}).$$

Si $k_1 + k_2 + \cdots$ n'est pas $\equiv 0$, la dernière somme est nulle ; elle est égale à n dans le cas contraire ; il reste de cette façon

$$\Sigma_h x_h^\lambda = n\text{A}\Sigma_{k_1 k_2 \ldots} \psi_{k_1 t} \psi_{k_2 t} \ldots = n\text{A}\Sigma_{k_1 k_2 \ldots} \psi_t^{(k_1+k_2+\ldots)} \varphi_{k_1}(\omega^t) \varphi_{k_2}(\omega^t) ;$$

la dernière valeur a été obtenue en appliquant l'équation (14) ; dans la somme, $k_1 + k_2 + \cdots$ doit être $\equiv 0$, et il s'ensuit, d'après une remarque faite, que $\psi_t^{k_1+k_2+\cdots}$ est une fonction rationnelle de ω^t ; on a donc

$$\Sigma x_h^\lambda = \text{R}(\omega^t),$$

où R est une fonction rationnelle ; le raisonnement précédent montre qu'elle garde la même forme quel que soit t ; elle est donc égale à

$$\frac{1}{n-1}[\text{R}(\omega) + \text{R}(\omega^2) + \cdots + \text{R}(\omega^{n-1})],$$

et c'est une fonction indépendante de ω, par suite rationnellement exprimable au moyen des coefficients de F et f_1.

Un raisonnement analogue montre que la somme $\Sigma x_{h+1} x_h^\lambda$ est rationnelle ; par suite la proposition est démontrée, et les formules (11) et (13) donnent toutes les racines des équations abéliennes de degré premier.

Une conséquence importante tirée par Kronecker de ce qui précède, et que nous nous contentons d'énoncer, est la suivante :

Les racines d'une équation abélienne de degré quelconque, à coefficients entiers, sont des fonctions rationnelles des racines de l'unité.

89. Appliquons ces considérations aux racines des équations abéliennes du troisième degré.

Sans nuire à la généralité, nous pouvons supposer que ψ_0, c'est-à-dire la somme des racines, est nulle, et faire entrer la fonction F de la formule (13) dans les facteurs du produit ; on a de cette façon

$$\psi_1 = f(\omega)^{\frac{1}{3}} f(\omega^2)^{\frac{2}{3}}, \qquad \psi_2 = f(\omega)^{\frac{2}{3}} f(\omega^2)^{\frac{1}{3}},$$

ou bien encore

$$\psi_1 = (a + b\sqrt{-3})^{\frac{1}{3}}(a - b\sqrt{-3})^{\frac{2}{3}},$$

$$\psi_2 = (a + b\sqrt{-3})^{\frac{2}{3}}(a - b\sqrt{-3})^{\frac{1}{3}},$$

où a et b sont rationnels. Les racines sont alors données par les équations

$$3x_0 = \psi_1 + \psi_2, \qquad 3x_1 = \omega^2\psi_1 + \omega\psi_2, \qquad 3x_2 = \omega\psi_1 + \omega^2\psi_2,$$

et les coefficients de l'équation, mise sous la forme $x^3 + px + q = 0$, ont pour valeurs

$$p = -\frac{\psi_1\psi_2}{3} = -\frac{a^2 + 3b^2}{3},$$

$$q = -\frac{\psi_1^3 + \psi_2^3}{27} = -\frac{2a(a^2 + 3b^2)}{27};$$

on retrouve les expressions déjà données au § 53 en remplaçant a et b par $\frac{9\lambda}{2}$ et $\frac{\mu}{2}$.

Les raisonnements que nous avons faits ne s'appliquent pas à l'équation du quatrième degré, puisque 4 n'est pas un nombre premier ; nous allons chercher directement la valeur des fonctions

$$\psi_k = x_0 + i^k x_1 + i^{2k} x_2 + i^{3k} x_3 \qquad (k = 0, 1, 2, 3),$$

d'où nous déduirons les racines par la formule (11).

Les fonctions $\frac{\psi_1\psi_2}{\psi_3}$ et $\frac{\psi_3\psi_2}{\psi_1}$ sont cycliques et s'expriment rationnellement au moyen des quantités connues et de la racine i de l'unité ; comme elles se transforment l'une dans l'autre par le changement de i en $-i$, on peut poser

$$\frac{\psi_1\psi_2}{\psi_3} = b(1 + di), \qquad \frac{\psi_3\psi_2}{\psi_1} = b(1 - di),$$

b et d étant rationnels, d'où l'on a

$$\psi_2^2 = b^2(1 + d^2), \qquad \frac{\psi_1^2}{\psi_3^2} = \frac{1 + di}{1 - di};$$

d'autre part $\frac{\psi_1\psi_3}{\psi_2^2}$ est aussi une fonction cyclique, et elle ne change pas lorsqu'on remplace i par $-i$, de sorte qu'on peut la représenter par $\frac{c}{2b^2}$; on en déduit

$$\psi_1\psi_3 = \frac{1}{2} c(1 + d^2),$$

et

$$\psi_1^4 = \frac{1}{4} c^2(1 + di)^3(1 - di).$$

Nous avons de cette façon ψ_1 en extrayant une racine quatrième, ψ_2 au moyen d'une racine carrée et ψ_3 en changeant dans ψ_1 i en $-i$; comme ψ_0 est un nombre rationnel qu'on peut désigner par a, on obtient finalement

$$4x_0 = a + b\sqrt{1 + d^2} + \sqrt{\frac{c}{2}(1 + di)\sqrt{1 + d^2}} + \sqrt{\frac{c}{2}(1 - di)\sqrt{1 + d^2}},$$

ou, en remplaçant la somme $\psi_1 + \psi_3$ par la racine carrée de son carré,

$$4x_0 = a + b\sqrt{1 + d^2} + \sqrt{c(1 + d^2 + \sqrt{1 + d^2})}.$$

Telle est l'expression, déjà donnée par Abel, d'une racine d'une équation abélienne du quatrième degré ; les autres s'en déduisent immédiatement en appliquant la formule (11). On vérifierait facilement que les fonctions symétriques et cycliques des racines sont rationnellement exprimables, quelles que soient les valeurs rationnelles de a, b, c, d.

CHAPITRE XI

DES ÉQUATIONS DE LA DIVISION DU CERCLE

---

90. Nous avons vu dans les chapitres précédents le rôle joué par les racines primitives de l'unité dans la résolution algébrique de certaines équations ; nous allons montrer que les équations dont elles dépendent rentrent dans la catégorie des équations abéliennes, et sont résolubles par radicaux ; nous entendons par là que les racines primitives de l'équation

$$x^m - 1 = 0$$

peuvent être calculées séparément au moyen de radicaux lorsqu'on suppose connues celles des équations binomes de degré moindre ; le calcul étant répété pour celles-ci, on voit comment les racines primitives de l'équation de degré m sont calculables par radicaux successifs.

C'est du reste l'étude approfondie faite par Gauss de la résolution des équations binomes qui a conduit Abel à celle des équations qui portent son nom ; nous suivrons ici une marche inverse en appliquant aux équations actuelles les résultats du chapitre précédent.

Remarquons d'abord que si $m = m_1 m_2 \ldots m_\nu$ est une décomposition du nombre m en facteurs premiers entre eux deux à deux, la recherche d'une racine primitive d'ordre m se ramène, comme on le sait, à celle d'une racine primitive de chacun des ordres $m_1, m_2, \ldots, m_\nu$, de sorte que si le nombre m décomposé en ses facteurs premiers est de la forme

$$m = p^\alpha q^\beta \ldots,$$

il suffit de calculer une racine primitive de chacune des équations

$$x^{p^\alpha} - 1 = 0, \qquad x^{q^\beta} - 1 = 0, \qquad \ldots$$

Pour la première par exemple, prenons une racine primitive ω_1 de l'équation

$$x^p - 1 = 0,$$

puis désignons par $\omega_2, \omega_3, \ldots, \omega_\alpha$ une racine de chacune des équations successives

$$x^p - \omega_1 = 0, \qquad x^p - \omega_2 = 0, \qquad \ldots, \qquad x^p - \omega_{\alpha-1} = 0;$$

leurs valeurs sont par exemple

$$\omega_2 = \omega_1^{\lambda_2}\sqrt[p]{\omega_1}, \qquad \omega_3 = \omega_1^{\lambda_3}\sqrt[p]{\omega_2}, \qquad \ldots, \qquad \omega_\alpha = \omega_1^{\lambda_\alpha}\sqrt[p]{\omega_{\alpha-1}};$$

je dis que le produit

$$\omega = \omega_1\omega_2\omega_3\ldots\omega_\alpha$$

est une racine primitive d'ordre p^α; en effet, on a d'abord $\omega^{p^\alpha} - 1 = 0$; il suffit de voir que le produit ω ne satisfait pas à l'équation $x^{p^{\alpha-1}} - 1 = 0$ qui possède toutes les racines non primitives de celle de degré p^α; or on a

$$\omega^{p^{\alpha-1}} = \omega_1,$$

qui est $\neq 1$, par suite ω est racine primitive de l'équation de degré p^α. On voit que le calcul de ω se ramène à celui de ω_1 et à l'extraction de $\alpha - 1$ racines successives d'indice p; dès lors il suffit de considérer le cas d'une équation binome de degré premier p.

91. Les racines de cette équation, autres que l'unité, sont primitives, et de la forme

$$\omega_1, \omega_1^2, \ldots, \omega_1^{p-1};$$

elles satisfont à l'équation

$$(1) \quad f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1 = 0,$$

appelée par Gauss « équation de la division du cercle pour le nombre p ».

Elle possède la propriété d'être irréductible (*). Supposons en effet qu'elle ne le soit pas, et que $f(x)$ soit le produit de deux polynomes entiers à coefficients rationnels; d'après une proposition rap-

(*) Comparer Netto, *Substitutionentheorie*, p. 174.

pelée au § 33, on peut admettre qu'ils sont à coefficients entiers; supposons que l'on ait

$$(2)\qquad f(x) = \varphi(x)\psi(x),$$

où φ et ψ ont leurs coefficients entiers; pour $x = 1$ on en tire

$$p = \varphi(1)\psi(1),$$

de sorte qu'un des nombres qui forment le second membre est égal à ± 1; soit $\varphi(1)$ ce nombre.

$\varphi(x)$ s'annulant pour une racine telle que ω_1, le produit

$$\varphi(x)\varphi(x^2)\ldots\varphi(x^{p-1})$$

s'annule pour $\omega_1, \omega_1^2, \ldots, \omega_1^{p-1}$, c'est-à-dire pour toutes les racines de l'équation (1) et est divisible par $f(x)$; en effectuant le calcul, on constate que le quotient a ses coefficients entiers, et en le représentant par $f_1(x)$, on a

$$\varphi(x)\varphi(x^2)\ldots\varphi(x^{p-1}) = f(x)f_1(x).$$

Si l'on fait dans cette identité $x = 1$, il vient

$$(\pm 1)^{p-1} = pf_1(1),$$

ce qui est impossible puisque $f_1(1)$ est un nombre entier; par suite l'équation (1) est irréductible.

92. C'est une équation abélienne, car si g est une racine primitive (mod. p), les racines $\omega_1, \omega_1^2, \ldots$ peuvent être représentées par

$$\omega,\ \omega^g,\ \omega^{g^2},\ \ldots,\ \omega^{g^{p-2}}$$

ou, en posant $\theta(\omega) = \omega^g$, par

$$\omega,\ \theta(\omega),\ \theta^2(\omega),\ \ldots,\ \theta^{p-2}(\omega);$$

on peut par suite leur appliquer la méthode du § 78. Si nous désignons par α une racine primitive de l'équation

$$x^{p-1} - 1 = 0,$$

la fonction cyclique

$$T_1 = \psi_1^{p-1} = \left(\omega + \alpha\omega^g + \cdots + \alpha^{p-2}\omega^{g^{p-2}}\right)^{p-1}$$

est rationnelle, ainsi que les produits

$$T_h = \psi_h\psi_1^{p-1-h} = \left(\omega + \alpha^h\omega^g + \ldots + \alpha^{h(p-2)}\omega^{g^{p-2}}\right)\left(\omega + \alpha\omega^g + \ldots + \alpha^{p-2}\omega^{g^{p-2}}\right)^{p-1-h},$$

de sorte que l'on a, en se reportant aux formules (8) du § cité,

$$\omega = \frac{1}{p-1}\left[-1 + \sqrt[p-1]{T_1} + \frac{T_2}{T_1}\left(\sqrt[p-1]{T_1}\right)^2 + \ldots + \frac{T_{p-2}}{T_1}\left(\sqrt[p-1]{T_1}\right)^{p-2}\right],$$

$$\omega^g = \frac{1}{p-1}\left[-1 + \alpha^{-1}\sqrt[p-1]{T_1} + \alpha^{-2}\frac{T_2}{T_1}\left(\sqrt[p-1]{T_1}\right)^2 + \ldots + \alpha^{-(p-2)}\frac{T_{p-2}}{T_1}\left(\sqrt[p-1]{T_1}\right)^{p-2}\right],$$

. . . .

Le calcul des racines ω, ω^g,... est ainsi ramené à celui d'un seul radical d'indice $p-1$ et à celui d'une racine primitive de l'équation binome de degré $p-1$.

Comme $f(x)$ et θ ont leurs coefficients réels, la détermination de $\sqrt[p-1]{T_1}$ se ramène, comme nous l'avons vu au § 79, à la division d'un angle ϑ en $p-1$ parties égales, et à l'extraction de la racine carrée d'une quantité connue U, qui est égale à la valeur absolue du produit réel

$$\psi_1\psi_{p-2}=\left(\omega+\alpha\omega^g+\ldots+\alpha^{p-2}\omega^{g^{p-2}}\right)\left(\omega+\alpha^{p-2}\omega^g+\alpha^{p-3}\omega^{g^2}+\ldots+\alpha\omega^{g^{p-2}}\right).$$

En effectuant le produit indiqué au second membre, on a

$$\begin{aligned}\psi_1\psi_{p-2} = &\left(\omega^2+\omega^{2g}+\ldots+\omega^{2g^{p-2}}\right)\\ &+\alpha\left(\omega^{1+g}+\omega^{(1+g)g}+\ldots+\omega^{(1+g)g^{p-2}}\right)\\ &+\alpha^2\left(\omega^{1+g^2}+\omega^{(1+g^2)g}+\ldots+\omega^{(1+g^2)g^{p-2}}\right)\\ &+\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

Les nombres 2, $1+g$, $1+g^2$, ..., $1+g^{p-2}$ sont, dans un ordre quelconque, congrus à $2, 3, \ldots, p-1, p$; le dernier p est donné par $1+g^{\frac{p-1}{2}}$, car $g^{\frac{p-1}{2}}$ est la seule puissance de g qui puisse être $\equiv -1 \pmod{p}$; on en conclut que chacune des puissances ω^2, ω^{1+g}, ..., $\omega^{1+g^{p-2}}$ représente une racine primitive de l'équation donnée, à l'exception de $\omega^{1+g^{\frac{p-1}{2}}}=1$, et que chaque parenthèse est identique à la somme des racines de $f(x)=0$, c'est-à-dire égale à -1, sauf le facteur de $\alpha^{\frac{p-1}{2}}$ qui est égal à $p-1$; on a donc

$$\psi_1\psi_{p-2} = -\left(1+\alpha+\alpha^2+\ldots+\alpha^{\frac{p-1}{2}}+\ldots+\alpha^{p-2}\right)+p\alpha^{\frac{p-1}{2}}.$$

Comme la première partie est nulle et que $\alpha^{\frac{p-1}{2}}=-1$, on a

$$\psi_1\psi_{p-2}=-p, \qquad U=p.$$

D'où ce résultat :

THÉORÈME I. — *Pour résoudre l'équation binome de degré p, il suffit : 1° de connaître une racine primitive de l'équation binome de degré $p-1$; 2° de diviser un angle que l'on peut alors construire en $p-1$ parties égales ; 3° de prendre la racine carrée du nombre p.*

93. Le problème est ainsi résolu, mais on peut opérer d'une autre manière, et prendre d'autres révolvantes que la fonction cyclique T_1, comme nous l'avons vu au § 81 ; si l'on pose

$$p-1 = m_1 m_2 \ldots m_\nu,$$

en décomposant $p-1$ en facteurs égaux ou inégaux, on peut déterminer ω en résolvant ν équations abéliennes successives de degrés $m_1, m_2, \ldots, m_\nu$ et adjoignant au domaine de rationalité les racines des équations binomes

$$x^{m_1}-1=0, \qquad x^{m_2}-1=0, \qquad \ldots, \qquad x^{m_\nu}-1=0.$$

α_1 étant une racine primitive de la première, on posera

$$\begin{aligned}
\chi_0 &= \omega + \omega^{g^{m_1}} + \omega^{g^{2m_1}} + \cdots,\\
\chi_1 &= \omega^{g} + \omega^{g^{m_1+1}} + \omega^{g^{2m_1+1}} + \cdots,\\
&\cdots\cdots\cdots\cdots\cdots\\
\chi_{m_1-1} &= \omega^{g^{m_1-1}} + \omega^{g^{2m_1-1}} + \omega^{g^{3m_1-1}} + \cdots,
\end{aligned}$$

et on formera la résolvante

$$T_1 = (\chi_0 + \alpha_1\chi_1 + \alpha_1^2\chi_2 + \cdots + \alpha_1^{m_1-1}\chi_{m_1-1})^{m_1},$$

qui s'exprime rationnellement au moyen de α_1 et des coefficients de l'équation donnée. On déterminera les inconnues χ au moyen de α_1 et de $\sqrt[m_1]{T_1}$; leurs valeurs sont données par des formules analogues à la formule (9) du § 81. Connaissant l'une d'elles, par exemple χ_0, on partagera les $\dfrac{m}{m_1}$ racines dont elle est la somme en m_2 séries, et l'on posera

$$\begin{aligned}
\varphi_0 &= \omega + \omega^{g^{m_1 m_2}} + \omega^{g^{2m_1 m_2}} + \cdots,\\
\varphi_1 &= \omega^{g^{m_1}} + \omega^{g^{m_1(m_2+1)}} + \omega^{g^{2m_1(m_2+1)}} + \cdots,\\
&\cdots\cdots\cdots\cdots\cdots\\
\varphi_{m_2-1} &= \omega^{g^{m_1(m_2-1)}} + \omega^{g^{2m_1(m_2-1)}} + \omega^{g^{3m_1(m_2-1)}} + \cdots;
\end{aligned}$$

la résolvante

$$R_1 = \left(\varphi_0 + \alpha_2\varphi_1 + \alpha_2^2\varphi_2 + \cdots + \alpha_2^{m_2-1}\varphi_{m_2-1}\right)^{m_2},$$

où α_2 est une racine primitive de l'équation $x^{m_2}-1=0$, s'exprime rationnellement au moyen des coefficients de l'équation donnée et de χ_0 ; on déterminera alors les inconnues φ au moyen de α_2 et de $\sqrt[m_2]{R_1}$ comme précédemment ; on continuera de la même manière en partageant les $\dfrac{m}{m_1 m_2}$ racines dont φ_0 par exemple est

la somme, en m_3 séries, et ainsi de suite. On peut dès lors énoncer le théorème suivant :

THÉORÈME II. — *Si p est un nombre premier, et si l'on décompose $p-1$ en un produit de la forme*

$$p-1 = m_1 m_2 \ldots m_\nu,$$

il suffit, pour résoudre l'équation binome de degré p et en déterminer une racine primitive : 1° de calculer une racine primitive de chacune des équations

$$x^{m_1}-1=0, \qquad x^{m_2}-1=0, \qquad \ldots, \qquad x^{m_\nu}-1=0\,;$$

2° de calculer des racines successives d'indices $m_1, m_2, \ldots, m_\nu$ de quantités s'exprimant chacune rationnellement au moyen des radicaux déjà formés précédemment et des racines primitives dont on vient de parler.

On applique ordinairement ce théorème en prenant pour $m_1, m_2, \ldots, m_\nu$ les facteurs égaux ou inégaux de $p-1$ décomposé en ses facteurs premiers ; il est cependant un choix particulier de ces nombres que nous allons mentionner.

Supposons que les diviseurs $m_1, m_2, \ldots, m_\nu$ de $p-1$ soient premiers entre eux deux à deux, sans être forcément premiers absolus ; considérons les fonctions analogues à χ_0, obtenues en remplaçant m_1 par $m_2, \ldots, m_\nu$, et désignons-les par

$$\chi_{01} = \omega + \omega^{g^{m_1}} + \omega^{g^{2m_1}} + \cdots,$$
$$\chi_{02} = \omega + \omega^{g^{m_2}} + \omega^{g^{2m_2}} + \cdots,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\chi_{0\nu} = \omega + \omega^{g^{m_\nu}} + \omega^{g^{2m_\nu}} + \cdots\,;$$

χ_{0h} s'exprime au moyen d'une racine primitive α_h de l'équation $x^{m_h}-1=0$ et d'un radical $\sqrt[m_h]{T_{1h}}$ portant sur une quantité qui dépend rationnellement de α_h.

Formons alors l'équation $f_h(x, \chi_{0h}) = 0$ dont dépendent les racines dont la somme est χ_{0h} ; ses coefficients sont des fonctions rationnelles de cette quantité ; toutes les équations analogues, obtenues en donnant à h les valeurs $1, 2, \ldots, \nu$, ont la racine commune ω et n'en ont aucune autre ; on obtiendra donc cette racine en cherchant le plus grand commun diviseur des polynomes f_h et en l'égalant à zéro ; la racine de ce commun diviseur, qui est du premier degré, est une fonction rationnelle des quantités $\chi_{01}, \chi_{02}, \ldots, \chi_{0\nu}$. On peut donc énoncer le corollaire suivant :

COROLLAIRE. — *Si les nombres $m_1, m_2, \ldots, m_\nu$ dont le produit est égal à $p-1$ sont premiers entre eux, une racine primitive de l'équation binome de degré p s'exprime rationnellement au moyen d'une racine primitive de chacune des équations binomes*

$$x^{m_1}-1=0, \qquad x^{m_2}-1=0, \qquad \ldots, \qquad x^{m_\nu}-1=0$$

et de radicaux d'indices $m_1, m_2, \ldots, m_\nu$ portant respectivement sur des fonctions rationnelles de ces racines.

Le cas le plus important est celui où les facteurs du nombre $p-1$ sont tous égaux à 2; le nombre premier p est de la forme 2^m+1, et il est nécessaire que m soit lui-même égal à 2^μ, car si l'on avait $m=2^\mu(2m'+1)$, le nombre

$$2^m+1=\left(2^{2^\mu}\right)^{2m'+1}+1$$

serait divisible par $2^{2^\mu}+1$ et ne serait pas premier. Les racines primitives des équations binomes auxiliaires sont égales à -1, et les radicaux successifs ont tous leur indice égal à 2. On a dans ce cas le résultat suivant :

THÉORÈME III. — *L'équation binome dont le degré est un nombre premier p de la forme $2^{2^\mu}+1$ est résoluble au moyen d'extractions de racines carrées successives.*

Pour $\mu=0, 1, 2, 3, 4,$ on a des nombres premiers qui sont

$$p=3, \quad 5, \quad 17, \quad 257, \quad 65537;$$

mais pour $\mu=5$, le nombre obtenu n'est pas premier, car

$$2^{2^5}+1=4294967297=641.6700417,$$

de sorte qu'on ne sait pas si la suite des nombres de la forme précédente contient un nombre limité ou illimité de nombres premiers.

94. Considérons le cas où l'on décompose le nombre $p-1$ en un produit de deux facteurs $m_1=2$ et $m_2=\frac{p-1}{2}$; nous devons poser

$$\chi_0=\omega+\omega^{g^2}+\omega^{g^4}+\cdots,$$

$$\chi_1=\omega^g+\omega^{g^3}+\omega^{g^5}+\cdots,$$

et former la résolvante

$$T_1=(\chi_0-\chi_1)^2.$$

T_1 s'exprime rationnellement au moyen des coefficients de l'équation ; on obtiendra sa valeur en remplaçant dans le produit $\psi_1\psi_{p-2}$

du § 92 α par -1, car on a $\alpha^{p-2} = -1$ et les deux facteurs de ce produit sont égaux à $\chi_0 - \chi_1$; nous avons de cette façon

$$T_1 = (-1)^{\frac{p-1}{2}} p.$$

Comme on a d'autre part $\chi_0 + \chi_1 = -1$, les deux inconnues χ_0 et χ_1 ont pour valeurs

$$\chi_0 = \frac{1}{2}\left[-1 + \sqrt{(-1)^{\frac{p-1}{2}} p}\right], \quad \chi_1 = \frac{1}{2}\left[-1 - \sqrt{(-1)^{\frac{p-1}{2}} p}\right].$$

Nous devons ensuite exprimer en fonction rationnelle des deux quantités précédentes les coefficients des équations

$$f_0(x) = (x - \omega)(x - \omega^{g^2})(x - \omega^{g^4}) \ldots = 0,$$
$$f_1(x) = (x - \omega^g)(x - \omega^{g^3})(x - \omega^{g^5}) \ldots = 0,$$

dont les racines entrent respectivement dans χ_0 et χ_1; un coefficient A de la première par exemple est une fonction entière à coefficients entiers de toutes les racines et a la forme

$$A = a_0 + a_1\omega + a_2\omega^g + a_3\omega^{g^2} + \cdots.$$

Je dis que l'on a $a_1 = a_3 = a_5 = \cdots$, et $a_2 = a_4 = \cdots$; en effet, A ne change pas lorsqu'on remplace ω par ω^{g^2}, de sorte que l'on a encore

$$A = a_0 + a_1\omega^{g^2} + a_2\omega^{g^3} + \cdots,$$

d'où l'on tire

$$(a_3 - a_1)\omega^{g^2} + (a_4 - a_2)\omega^{g^3} + \cdots = 0;$$

cette équation, que l'on peut réduire au degré $p-2$ par rapport à la racine ω appartenant à l'équation irréductible $f(x) = 0$, ne peut avoir lieu que si les coefficients sont tous nuls, c'est-à-dire si l'on a $a_1 = a_3 = \cdots$, et $a_2 = a_4 = \cdots$, ce que nous voulions démontrer.

Il résulte de là que le coefficient A est une fonction linéaire à coefficients entiers de χ_0 et de χ_1, ou bien, en vertu de la relation $\chi_0 + \chi_1 = -1$, une fonction de même nature de χ_0; par suite $f_0(x)$ peut se mettre sous la forme

$$f_0(x) = P + Q\chi_0,$$

où P et Q sont des polynomes entiers à coefficients entiers; on aurait $f_1(x)$ en changeant χ_0 en χ_1, ce qui donne

$$f_1(x) = P + Q\chi_1;$$

en remplaçant χ_0 et χ_1 par leurs valeurs, on peut écrire

$$f_0(x)=\frac{1}{2}\left[X+\sqrt{(-1)^{\frac{p-1}{2}}pY}\right],\qquad f_1(x)=\frac{1}{2}\left[X-\sqrt{(-1)^{\frac{p-1}{2}}pY}\right],$$

où X et Y sont encore des polynomes entiers à coefficients entiers.

Remarquons que le premier membre $f(x)$ de l'équation (1) est égal au produit $f_0(x)f_1(x)$; on a donc l'identité

$$f(x) = x^{p-1}+x^{p-2}+\cdots+x+1 = \frac{1}{4}\left[X^2-(-1)^{\frac{p-1}{2}}pY^2\right],$$

d'où le résultat suivant :

THÉORÈME IV. — *Lorsque* p *est un nombre premier, on a identiquement*

$$4(x^{p-1}+x^{p-2}+\cdots+x+1) = X^2-(-1)^{\frac{p-1}{2}}pY^2,$$

X *et* Y *étant des polynomes entiers à coefficients entiers.*

95. La résolution de l'équation binome de degré m est équivalente à la solution de ce problème : Diviser la circonférence du cercle en m parties égales ; cela résulte de ce que si ω est une racine de l'équation binome égale à $\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$, on a

$$\omega^k = \cos\frac{2k\pi}{m}+i\sin\frac{2k\pi}{m},$$

$$2\cos\frac{2k\pi}{m} = \omega^k+\omega^{m-k},$$

$$2i\sin\frac{2k\pi}{m} = \omega^k-\omega^{m-k},$$

$$\sin\frac{2k\pi}{m} = \sqrt{1-\left(\frac{\omega^k+\omega^{m-k}}{2}\right)^2};$$

par suite la connaissance des racines ω de l'équation binome entraîne celle des lignes trigonométriques des arcs égaux à $\frac{2k\pi}{m}$ et celle des points de division de la circonférence partagée en m parties égales, et réciproquement. On peut donc énoncer les résultats suivants :

Pour inscrire dans une circonférence un polygone régulier d'un nombre premier p *de côtés, il suffit de diviser la circonférence en* $p-1$ *parties égales, de diviser un arc, que l'on peut alors cons-*

truire, en $p-1$ *parties égales, et de prendre une moyenne proportionnelle entre le rayon et* p *fois le rayon.*

Si les facteurs premiers de $p-1$ *sont* $m_1, m_2, \ldots, m_\nu$, *il suffit aussi de partager la circonférence en* $m_1, m_2, \ldots, m_\nu$ *parties égales et de construire des quantités exprimées par des radicaux successifs d'indices* $m_1, m_2, \ldots, m_\nu$.

Il est toujours possible d'inscrire dans une circonférence, avec la règle et le compas, un polygone régulier dont le nombre des côtés est un nombre premier de la forme $2^{2^\mu}+1$.

Considérons le cas de $p=5$ et choisissons pour g le nombre 2; nous avons

$$g^0 \equiv 1, \qquad g \equiv 2, \qquad g^2 \equiv 4, \qquad g^3 \equiv 3 \qquad (\text{mod. } 5);$$

en posant

$$\chi_0 = \omega + \omega^{g^2} = \omega + \omega^4,$$

$$\chi_1 = \omega^g + \omega^{g^3} = \omega^2 + \omega^3,$$

χ_0 et χ_1 sont racines de l'équation

$$\chi^2 + \chi - 1 = 0.$$

Si l'on ne fixe pas la valeur que l'on prend pour ω, le choix des racines χ_0, χ_1 est indifférent, mais si l'on se donne

$$\omega = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5},$$

il faut prendre

$$\chi_0 = \frac{-1+\sqrt{5}}{2}, \qquad \chi_1 = \frac{-1-\sqrt{5}}{2}.$$

Ensuite, on a

$$\omega + \omega^4 = \chi_0, \qquad \omega\omega^4 = 1,$$

$$\omega^2 + \omega^3 = \chi_1, \qquad \omega^2\omega^3 = 1,$$

de sorte qu'on a à résoudre les équations

$$x^2 - \chi_0 x + 1 = 0,$$

$$x^2 - \chi_1 x + 1 = 0,$$

et alors on a, en choisissant comme il convient le signe du coefficient de i,

$$\omega = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Pour $p=17$, le nombre $g=6$ est une racine primitive ; il fournit comme restes de $g^0, g^1, \ldots$ les nombres

1, 6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3.

Les sommes

$$\chi_0 = \omega + \omega^2 + \omega^4 + \omega^8 + \omega^{16} + \omega^{15} + \omega^{13} + \omega^9,$$

$$\chi_1 = \omega^6 + \omega^{12} + \omega^7 + \omega^{14} + \omega^{11} + \omega^5 + \omega^{10} + \omega^3$$

sont les racines de

$$\chi^2 + \chi - 4 = 0.$$

Si l'on choisit pour ω la valeur

$$\omega = \cos\frac{2\pi}{17} + i \sin\frac{2\pi}{17},$$

il faut prendre, comme on le voit facilement,

$$\chi_0 = \frac{-1+\sqrt{17}}{2}, \qquad \chi_1 = \frac{-1-\sqrt{17}}{2}.$$

On a ensuite, au moyen de χ_0 et χ_1,

$$\varphi_0 = \omega + \omega^4 + \omega^{16} + \omega^{13}, \qquad \varphi'_0 = \omega^6 + \omega^7 + \omega^{11} + \omega^{10},$$

$$\varphi_1 = \omega^2 + \omega^8 + \omega^{15} + \omega^9, \qquad \varphi'_1 = \omega^{12} + \omega^{14} + \omega^5 + \omega^3,$$

qui sont racines de

$$\varphi^2 - \chi_0\varphi - 1 = 0, \qquad \varphi'^2 - \chi_1\varphi' - 1 = 0;$$

leurs valeurs sont

$$\varphi_0 = \frac{\chi_0}{2} + \sqrt{\frac{\chi_0^2}{4} + 1}, \qquad \varphi'_0 = \frac{\chi_1}{2} - \sqrt{\frac{\chi_1^2}{4} + 1},$$

$$\varphi_1 = \frac{\chi_0}{2} - \sqrt{\frac{\chi_0^2}{4} + 1}, \qquad \varphi'_1 = \frac{\chi_1}{2} + \sqrt{\frac{\chi_1^2}{4} + 1}.$$

En se limitant à φ_0, et posant

$$\sigma_0 = \omega + \omega^{16}, \qquad \sigma_1 = \omega^4 + \omega^{13},$$

on a

$$\sigma^2 - \varphi_0\sigma + \varphi'_1 = 0,$$

ou encore, en exprimant φ'_1 au moyen de φ_0,

$$\sigma^2 - \varphi_0\sigma + \frac{\varphi_0 - 1}{\varphi_0 + 1} = 0,$$

qui donne

$$\sigma_0 = \frac{\varphi_0}{2} + \sqrt{\frac{\varphi_0^2}{4} - \varphi'_1}, \qquad \sigma_1 = \frac{\varphi_0}{2} - \sqrt{\frac{\varphi_0^2}{4} - \varphi'_1}.$$

Enfin ω et ω^{16} sont les racines de

$$x^2 - \sigma_0 + 1 = 0,$$

de sorte que l'on a

$$\omega = \frac{\sigma_0}{2} + i\sqrt{1 - \frac{\sigma_0^2}{4}}.$$

Il est facile de tirer de là une construction du polygone de 17 côtés inscrit dans la circonférence (*).

96. Les mêmes considérations s'appliqueraient à l'équation dont dépend directement la recherche de $\cos \frac{2\pi}{m}$; on l'obtient en exprimant la fonction

$$V_m = x^m + \frac{1}{x^m}$$

au moyen de

$$z = x + \frac{1}{x}$$

et posant $x = \cos a + i \sin a$; on a ainsi $z = 2\cos a$, $V_m = 2\cos ma$, et l'on obtient, par un calcul employé dans la théorie des équations réciproques,

$$(3) \qquad 2\cos ma = z^m - mz^{m-2} + \frac{m(m-3)}{1.2} z^{m-4} - \dots$$

Il suffit de faire $a = \frac{2\pi}{m}$ pour avoir l'équation ayant pour racines

$$(4) \quad 2\cos\frac{2\pi}{m}, \quad 2\cos\frac{4\pi}{m}, \quad \dots, \quad 2\cos\frac{2(m-1)\pi}{m}, \quad 2\cos\frac{2m\pi}{m}.$$

C'est une équation abélienne, car si l'on représente par

$$x_1, \ x_2, \ \dots, \ x_{m-1}, \ x_m$$

les m racines précédentes, x_k est une fonction de x_1 donnée précisément par la formule (3) où l'on remplace m par k, a par $\frac{2\pi}{m}$ et z par x_1; de plus si l'on pose pour toute valeur de k $x_k = \theta_k(x_1)$, on a

$$(5) \qquad \theta_h\theta_k(x_1) = \theta_k\theta_h(x_1) = 2\cos\frac{2hk\pi}{m},$$

de sorte que les fonctions θ sont échangeables et l'équation est abélienne. On pourrait lui appliquer les procédés que nous avons

(*) Consulter à ce sujet SERRET, *Algèbre Supérieure*, t. II, p. 565; NETTO, *Substitutionentheorie*, p. 183; BACHMANN, *Die Lehre von der Kreistheilung*.

indiqués pour la résoudre par radicaux, mais cette méthode de résolution serait au fond identique à la recherche des racines m^{es} de l'unité.

Il est préférable de remarquer, dans le cas où m est un nombre impair égal à $2\mu+1$, que les racines de la suite (4) sont l'une égale à $+1$ et les autres deux à deux égales et de signes contraires. On partira de l'équation binome

$$x^{2\mu+1}-1=0$$

ou plutôt de la suivante

$$\frac{x^{2\mu+1}-1}{x-1}=x^{2\mu}+x^{2\mu-1}+\cdots+x+1=0 \tag{6}$$

et on lui appliquera la méthode de réduction des équations réciproques, en formant l'équation ayant pour racine $z=x+\frac{1}{x}$; en se reportant à la formule (3) qui donne V_m, on a à calculer

$$U_\mu=V_\mu+V_{\mu-1}+\cdots+V_1+1,$$

ce qui donne, en égalant à zéro le résultat,

$$U_\mu=z^\mu+z^{\mu-1}-(\mu-1)z^{\mu-2}-(\mu-2)z^{\mu-3}+\frac{(\mu-2)(\mu-3)}{1.2}z^{\mu-4}+\ldots=0.$$

Cette équation, qui admet pour racines les valeurs distinctes de la suite (4) autres que l'unité, est encore une équation abélienne, d'après la propriété exprimée par l'équation (5) ; elle est alors résoluble par radicaux.

Dans le cas où $m=2\mu+1$ est un nombre premier, on reconnaît que les racines sont de la forme suivante, en désignant par λ une racine primitive (mod. m) (*).

$$2\cos\frac{2\pi}{m},\quad 2\cos\frac{2\lambda\pi}{m},\quad 2\cos\frac{2\lambda^2\pi}{m},\quad \ldots,\quad 2\cos\frac{2\lambda^{\mu-1}\pi}{m}; \tag{7}$$

en effet, les puissances λ^0, λ^1, λ^2, ..., $\lambda^{\mu-1}$ sont des nombres distincts de la suite $1, 2, 3, \ldots, m-1$; il suffit de faire voir que les μ cosinus précédents sont distincts pour affirmer que ce sont les racines de l'équation $U_\mu=0$.

Or si l'on avait par exemple

$$\cos\frac{2\lambda^h\pi}{m}=\cos\frac{2\lambda^k\pi}{m} \qquad (h<k\,;\ h,\ k\leqslant\mu-1),$$

(*) Comparer Serret, *Algèbre supérieure*, t. II, p. 560.

on en déduirait

$$\frac{2\lambda^k\pi}{m} \pm \frac{2\lambda^h\pi}{m} = 2\pi, \qquad \lambda^k \pm \lambda^h = m,$$

d'où

$$\lambda^h(\lambda^{k-h} \pm 1) = m;$$

le nombre premier m ne divisant pas λ^h serait un diviseur de $\lambda^{k-h}+1$ ou de $\lambda^{k-h}-1$, c'est-à-dire du produit $\lambda^{2k-2h}-1$ de ces deux nombres ; mais cela est impossible, puisque $2k-2h$ est inférieur à $m-1$.

On voit donc que les racines de $U_\mu = 0$ sont données par la suite (7) ; si l'on représente la première par x_1, et par $\theta(x_1)$ la fonction rationnelle qui représente la valeur de la seconde $2\cos\frac{2\lambda\pi}{m}$, on constate que les nombres de cette suite peuvent être représentés par

$$x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots,\ \theta^{\mu-1}(x_1);$$

ils sont les racines d'une équation abélienne simple, et nous avons vu précédemment comment on les exprime au moyen de radicaux.

Dans le cas où m est un nombre pair, de la forme $2\mu+2$, les racines de la suite (4) sont l'une égale à $+1$, une autre égale à -1, et les 2μ autres sont encore égales et de signes contraires ; elles sont les racines de l'équation obtenue en remplaçant dans l'équation suivante

$$(8) \qquad \frac{x^{2\mu+2}-1}{x^2-1} = x^{2\mu} + x^{2\mu-2} + \cdots + x^2 + 1 = 0$$

$x + \frac{1}{x}$ par z ; or si l'on pose $x^2 = t$, t est fourni par une équation de degré μ analogue à (6) ; dans le cas où μ est pair, on lui applique la méthode précédente, et z est donné par la relation

$$z^2 - 2 = x^2 + \frac{1}{x^2} = t + \frac{1}{t};$$

si au contraire μ est impair, l'équation en t tirée de (8) a une racine égale à -1, et l'on est ramené à une équation de degré $\mu-1$.

CHAPITRE XII

DES ÉQUATIONS RÉSOLUBLES IRRÉDUCTIBLES DE DEGRÉ PREMIER

97. Nous avons vu que les équations abéliennes sont résolubles algébriquement après adjonction au domaine de rationalité de certaines racines de l'unité ; elles sont caractérisées par cette propriété qu'une fonction cyclique des racines est rationnellement connue ; nous allons généraliser et rechercher quelles sont toutes les équations irréductibles résolubles de degré premier, en suivant la méthode indiquée par Kronecker dans ses leçons sur la théorie des équations algébriques professées à l'Université de Berlin, et reproduites en partie dans les *Monatsberichte* (3 mars 1879).

Nous considérons d'abord une équation

$$(1) \qquad f(x, \mathrm{R}, \mathrm{R}', \mathrm{R}'', \ldots) = 0$$

de degré premier n, dont les coefficients font partie d'un domaine de rationalité $(\mathrm{R}, \mathrm{R}', \mathrm{R}'', \ldots)$, et irréductible dans ce domaine ; comme au chapitre V, nous représenterons ses racines par $x_0, x_1, \ldots, x_{n-1}$. Nous allons d'abord étudier l'effet produit sur cette équation par l'adjonction au domaine d'une ou de plusieurs fonctions cycliques de ses racines.

En nous reportant à ce que nous avons dit sur les fonctions cycliques et métacycliques de plusieurs variables (chapitre V), nous n'avons à considérer pour n premier que les fonctions cycliques simples. Si l'on adjoint au domaine de rationalité une fonction cyclique particulière, toutes les racines de l'équation donnée s'expriment rationnellement au moyen de l'une d'elles dans le nouveau

domaine (§ 26) ; si donc une des racines s'exprime rationnellement, il en est de même des autres, et l'équation devient réductible, le premier membre étant décomposable en n facteurs du premier degré rationnels.

On peut montrer du reste que si le premier membre $f(x, R, R', R'', \ldots)$ se décompose en plusieurs facteurs irréductibles lorsqu'on adjoint au domaine une fonction cyclique $\gamma(x_0, x_1, \ldots, x_{n-1})$, ce ne peut être qu'en facteurs linéaires ; si l'on a en effet par exemple un facteur irréductible

$$\varphi(x, \gamma, R, R', \ldots) = (x - x_0)(x - x_1)(x - x_2)\ldots,$$

que l'on peut encore écrire, en exprimant $x_1, x_2, \ldots$ au moyen de x_0,

$$(x - x_0)[x - \theta_1(x_0, \gamma)][x - \theta_2(x_0, \gamma)]\ldots,$$

et un autre φ_1 contenant une autre racine x_h, la substitution du groupe cyclique auquel appartient γ et remplaçant x_0 par x_h ne change pas la valeur de φ et la transforme en φ_1 ; de cette façon chacun des facteurs irréductibles a le même degré et ne peut être que du premier degré, puisque n est premier.

Ainsi donc, après l'adjonction au domaine de rationalité d'une fonction cyclique particulière, l'équation reste irréductible ou se trouve décomposée en facteurs linéaires, c'est-à-dire résolue.

98. Il y a $(n-1)!$ valeurs algébriquement conjuguées d'une fonction cyclique, correspondant à $(n-2)!$ groupes distincts et appartenant $n-1$ à $n-1$ au même groupe ; il est impossible que l'équation se trouve résolue lorsqu'on adjoint une fonction appartenant à chacun des $(n-2)!$ groupes distincts, et *il existe au moins une fonction cyclique dont l'adjonction laisse l'équation irréductible.*

En effet, supposons pour plus de généralité que l'équation donnée soit spéciale et possède un groupe G auquel appartient algébriquement et numériquement une fonction $\varphi(x_0, x_1, \ldots, x_{n-1})$ et soit $\gamma_1(x_0, x_1, \ldots, x_{n-1})$ une fonction cyclique dont l'adjonction rend l'équation réductible en facteurs linéaires

$$f(x) = [x - R_0(\varphi, \gamma_1)][x - R_1(\varphi, \gamma_1)]\ldots$$

Formons le produit

$$F(x) = \Pi_\alpha[x - R_0(\varphi, \gamma_\alpha)]$$

étendu à toutes les valeurs algébriquement distinctes que prend γ_1 pour toutes les substitutions du groupe G; c'est une fonction appartenant au groupe de l'équation, et exprimable rationnellement; l'équation $F(x) = 0$ ayant une racine commune avec la proposée, $F(x)$ est divisible par $f(x)$ qui est irréductible, et se décompose en général en plusieurs facteurs dont l'un est $f(x)$; si

$$f(x) = [x - R_0(\varphi, \gamma_1)][x - R_0(\varphi, \gamma_\alpha)]\ldots,$$

$$f_1(x) = [x - R_0(\varphi, \gamma_\beta)][x - R_0(\varphi, \gamma_\delta)]\ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

sont les facteurs irréductibles de $F(x)$, les substitutions du groupe G doivent transformer $f(x)$ dans chacun des autres facteurs, et comme elles laissent $f(x)$ invariable, tous les facteurs sont identiques, de sorte que l'on a

$$F(x) = f(x)^\lambda;$$

on en conclut que le nombre des valeurs algébriquement distinctes de γ_1 entrant dans le produit $F(x)$ est égal à λn, et l'adjonction de chacune d'elles produit une décomposition de $f(x)$, c'est-à-dire la résolution de l'équation proposée.

S'il y a d'autres valeurs algébriquement distinctes des λn précédentes parmi les $(n-1)!$ valeurs possibles de γ_1, produisant une réduction de $f(x)$, un raisonnement analogue montre qu'on peut les ranger en séries distinctes, contenant chacune un nombre de fonctions multiple de n, celles de chaque série se déduisant de l'une d'entre elles par les substitutions de G; comme $(n-1)!$ n'est pas divisible par n, on voit qu'il y aura au moins une fonction cyclique des racines dont l'adjonction laisse l'équation irréductible.

Soit $\gamma(x_0, x_1, \ldots, x_{n-1})$ une telle fonction laissant $f(x)$ irréductible; supposons qu'elle appartienne à un groupe cyclique tel que

$$C = [S_1 = (x_0 x_1 \ldots x_{n-1}),\quad S^2, \ldots, S^{n-1},\quad S^n = 1];$$

le groupe G de l'équation doit contenir C comme sous-groupe, ou lui être identique. Supposons en effet que cela n'ait pas lieu; en adjoignant au domaine de rationalité la fonction γ, la fonction $u\gamma + v\varphi$, où φ appartient au groupe G, est rationnelle dans le nouveau domaine, et appartient au groupe G' formé des substitutions communes à C et à G; l'ordre de ce groupe G' étant diviseur de n ne peut être l'unité, car l'équation serait résoluble, la fonc-

tion de Galois devenant rationnellement exprimable ; il ne peut être que n, et G doit se confondre avec C ou le contenir comme sous-groupe, de sorte que l'on peut énoncer le théorème suivant :

THÉORÈME I. — *Le groupe d'une équation irréductible de degré premier est un groupe cyclique ou doit contenir au moins un tel groupe comme sous-groupe.*

Il renferme le groupe de toute fonction cyclique dont l'adjonction laisse l'équation irréductible.

99. Supposons maintenant que l'équation irréductible

$$(1) \qquad f(x, R', R'', R''', \ldots) = 0,$$

dont les coefficients font partie du domaine défini par les paramètres indépendants $R', R'', \ldots$, et dont le degré n est premier, soit résoluble algébriquement.

Considérons une fonction cyclique telle que $\gamma_1(x_0, x_1, \ldots, x_{n-1})$ appartenant au groupe C_1 dérivé de la substitution

$$S_1 = | z \quad z+1 | \qquad (\text{mod. } n)$$

et de ses puissances ; nous avons vu que parmi les $(n-1)!$ groupes auxquels appartiennent les valeurs conjuguées de γ_1, il en existe $n-1$ identiques à C_1 ; ce sont les groupes $C_1, C_2, \ldots, C_{n-1}$ dérivés respectivement de

$$S_1\Sigma_t = | z \quad tz+1 | \quad (\text{mod. } n) \quad (t = 1, 2, \ldots, n-1) ;$$

les autres groupes se partagent de même en séries de $n-1$ groupes identiques ; on les obtient en laissant dans C_1 les éléments x_0 et x_1 invariables et effectuant sur les $n-2$ autres $x_2, x_3, \ldots, x_{n-1}$ toutes les substitutions possibles. A ces $(n-2)!$ groupes appartiennent les valeurs conjuguées que nous désignerons par

$$\gamma_1, \gamma_2, \ldots, \gamma_{(n-2)!}.$$

Adjoignons au domaine de rationalité chacune de ces fonctions cycliques et désignons par

$$f(x, \gamma_1) = 0, \qquad f(x, \gamma_2) = 0, \qquad \ldots, \qquad f(x, \gamma_{(n-2)!}) = 0$$

ce que devient l'équation donnée après chacune de ces adjonctions ; nous allons montrer qu'une seule de ces équations reste irréductible, ce que nous énoncerons sous la forme suivante :

Théorème II. — *Une équation irréductible et résoluble de degré premier ne peut rester irréductible par l'adjonction de plus d'une fonction cyclique.*

Je suppose que l'équation (1) soit résoluble et reste irréductible lorsqu'on adjoint au domaine deux fonctions cycliques

$$(2) \qquad \gamma_1(x_0, x_1, \ldots, x_{n-1}),$$

$$(3) \qquad \gamma_i(x_{i_0}, x_{i_1}, \ldots, x_{i_{n-1}}),$$

appartenant à deux groupes différents C_1 et C_i dérivés respectivement des substitutions

$$S_1 = (x_0 x_1 \ldots x_{n-1}),$$

$$S_i = (x_{i_0} x_{i_1} \ldots x_{i_{n-1}})$$

et de leurs puissances ; on peut toujours supposer que dans S_i les deux premiers éléments x_{i_0} et x_{i_1} sont identiques à x_0 et x_1.

En nous reportant à la chaîne d'équations (2) du § 64, la première équation

$$(4) \qquad V_\nu^{p_\nu} = F_\nu(R', R'', \ldots)$$

est une relation entre les racines $x_0, x_1, \ldots, x_{n-1}$ de l'équation (1) lorsqu'on remplace V_ν par sa valeur en fonction de ces racines et des racines de l'unité, et l'on sait qu'elle reste satisfaite lorsqu'on effectue sur les racines les substitutions du groupe de l'équation (§ 47). D'après le théorème I, le premier membre de l'équation (4) reste invariable pour les substitutions des groupes cycliques C_1 et C_i auxquels appartiennent les fonctions (2) et (3), par suite, si l'on écrit la fonction V_ν sous la forme

$$V_\nu(x_{i_0}, x_{i_1}, \ldots, x_{i_k}, \ldots, x_{i_{n-1}}),$$

lorsqu'on augmente chaque nombre k d'une unité, ou bien chaque indice i_k d'une unité. Comme les nouvelles valeurs de V_ν ne diffèrent de la première que par une racine p_ν^e de l'unité, on aura, en désignant par ω une racine primitive de l'équation $x^{p_\nu} - 1 = 0$,

$$(5) \qquad V_\nu(\ldots x_{i_k} \ldots) = \omega^r V_\nu(\ldots x_{i_{k+1}} \ldots) = \omega^s V_\nu(\ldots x_{i_k+1} \ldots)$$

et, en répétant respectivement a et b fois ces substitutions,

$$V_\nu(\ldots x_{i_k} \ldots) = \omega^{ar} V_\nu(\ldots x_{i_{k+a}} \ldots) = \omega^{bs} V_\nu(\ldots x_{i_k+b} \ldots).$$

Pour a et b égaux à n, on doit avoir $nr \equiv 0$ et $ns \equiv 0 \pmod{p_\nu}$, puisque la fonction V_ν reprend sa valeur primitive. On peut tou-

jours supposer, comme nous l'avons dit, que $i_0 = 0$ et $i_1 = 1$; en donnant à b la valeur i_a, on obtient

$$\omega^{ar} V_\nu(\ldots x_{i_{k+a}} \ldots) = \omega^{i_a s} V_\nu(\ldots x_{i_k + i_a} \ldots),$$

d'où la relation

$$(6) \qquad V_\nu(\ldots x_{i_{k+a}} \ldots) = \omega^{(i_a s - ar)} V_\nu(\ldots x_{i_k + i_a} \ldots).$$

Si l'on considère la substitution

$$\Sigma = \begin{pmatrix} i_a & i_{a+1} & \ldots & i_{a+k} & \ldots \\ i_a + i_0 & i_a + i_1 & \ldots & i_a + i_k & \ldots \end{pmatrix}$$

remplaçant i_{k+a} par $i_k + i_a$, lorsque k varie de 0 à $n-1$, elle laisse invariable i_a, puisque $i_0 = 0$, et ne porte que sur $n-1$ éléments; son ordre, que nous désignerons par t, divise $(n-1)!$ et est premier avec n; après t applications successives de Σ aux deux membres de la formule (6), on obtient au second membre la valeur primitive de la fonction V_ν, de sorte que l'on a

$$\omega^{t(i_a s - ar)} = 1,$$

$$t(i_a s - ar) \equiv 0 \qquad (\text{mod. } p_\nu).$$

Considérons alors les trois congruences

$$nr \equiv 0, \qquad ns \equiv 0, \qquad t(i_a s - ar) \equiv 0 \qquad (\text{mod. } p_\nu).$$

Si r et s ne sont pas $\equiv 0$, il faut que $p_\nu = n$, et comme t est premier avec n, que $i_a s \equiv ar$ pour toute valeur de a; en particulier, pour $a = 1$ on a $i_a = 1$, d'où $s \equiv r$ et par suite $i_a \equiv a$ quel que soit a; mais cela est impossible puisque les substitutions fondamentales S_1 et S_i des groupes auxquels appartiennent les fonctions (2) et (3) sont distinctes.

Il faut alors que r et s soient $\equiv 0$; l'équation (5) montre dans ce cas que la fonction V_ν est, comme $V_\nu^{p_\nu}$, invariable pour les deux groupes cycliques C_1 et C_i; en passant à l'équation suivante

$$V_{\nu-1}^{p_{\nu-1}} = F_{\nu-1}(V_\nu, R', R'', \ldots),$$

le second membre appartient à la fois à ces deux groupes, et le même raisonnement montre que $V_{\nu-1}$ jouit de la même propriété; on peut continuer ainsi jusqu'à la racine x_0 et l'on voit qu'elle s'exprime rationnellement au moyen de γ_1 ou de γ_i; mais cela est impossible car $f(x)$ aurait alors un facteur $x - x_0$ rationnellement exprimable dans le domaine primitif auquel on adjoindrait γ_1 ou γ_i,

et l'équation (1) ne resterait pas irréductible après adjonction de γ_1 ou de γ_i contrairement aux hypothèses faites sur ces fonctions, par suite le théorème est démontré. On en déduit le corollaire suivant.

Corollaire. — *Si le groupe d'une équation irréductible de degré premier contient comme sous-groupes deux groupes cycliques distincts, l'équation n'est pas résoluble algébriquement.*

100. Nous allons démontrer la réciproque : *Toute équation irréductible de degré premier est résoluble algébriquement si parmi les $(n-2)!$ groupes cycliques distincts, il n'en existe qu'un dont les fonctions laissent, après leur adjonction, l'équation irréductible.*

Soit $\gamma_1(x_0, x_1, \ldots, x_{n-1})$ une fonction cyclique jouissant de cette propriété de laisser, apres son adjonction, l'équation irréductible ; on peut supposer les indices des racines choisis de façon que cette fonction reste invariable pour la substitution

$$S_1 = (x_0 x_1 x_2 \ldots x_{n-1})$$

et ses puissances ; il existe $n-1$ valeurs conjuguées de γ_1 s'exprimant rationnellement au moyen de l'une d'elles, et leurs fonctions symétriques et cycliques dans un certain ordre appartiennent au groupe métacyclique

$$(M) \quad |z \quad az+b| \quad (\text{mod. } n) \quad \begin{pmatrix} a = 1, 2, \ldots, n-1 \\ b = 0, 1, 2, \ldots, n-1 \end{pmatrix}.$$

Je dis que les fonctions appartenant à ce groupe sont rationnellement exprimables au moyen des éléments du domaine de rationalité.

Considérons l'équation $F(\gamma) = 0$ de degré $(n-1)!$ ayant pour racines les $(n-1)!$ valeurs conjuguées de γ_1 ; désignons par $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$ celles qui appartiennent au même groupe ; un facteur irréductible de $F(\gamma)$ ne peut s'annuler à la fois pour une des $n-1$ valeurs précédentes et pour une des autres, par exemple γ_n, car si

$$F_1(\gamma) = (\gamma - \gamma_1)(\gamma - \gamma_n) \ldots$$

est un tel facteur irréductible, une de ses racines γ_n produit par son adjonction au domaine de rationalité une réduction de $f(x, R', R'', \ldots)$, il en est alors de même des autres, comme nous l'avons vu au § 39, et en particulier de γ_1, ce qui est impossible.

Par suite les valeurs $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$ doivent entrer, à l'exclusion des autres, dans un ou plusieurs facteurs irréductibles de $F(\gamma)$, de sorte que le produit

$$(\gamma - \gamma_1)(\gamma - \gamma_2)\ldots(\gamma - \gamma_{n-1})$$

a ses coefficients rationnels ; par suite les fonctions appartenant au groupe M font partie du domaine de rationalité.

Mais nous avons vu au § 28 que les fonctions $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$ sont telles qu'une fonction cyclique particulière de ces valeurs appartienne au groupe métacyclique ; par suite on peut, dans le cas actuel, les déterminer en résolvant une équation abélienne de degré $n - 1$; une nouvelle équation abélienne de degré n donne les racines de l'équation proposée, qui se trouve ainsi résolue algébriquement. C'est aussi ce que nous avons vu en exposant les recherches de Lagrange (§ 62). On peut énoncer le théorème suivant :

Théorème III. — *La condition nécessaire et suffisante pour qu'une équation irréductible de degré premier soit résoluble algébriquement est qu'il existe une fonction métacyclique faisant partie du domaine de rationalité ; la résolution de l'équation dépend alors en général de deux équations abéliennes successives.*

Il est évident que les équations abéliennes rentrent comme cas particulier dans la catégorie précédente.

Corollaire. — *Le groupe d'une équation irréductible de degré premier résoluble algébriquement est le groupe métacyclique ou un de ses sous-groupes.*

101. Nous avons démontré au § 31 que chacune des quantités $x_0, x_1, \ldots, x_{n-1}$ est une fonction rationnelle de deux d'entre elles et d'une fonction métacyclique ; on peut donc énoncer le résultat suivant :

Théorème IV. — *Chacune des racines d'une équation irréductible et résoluble de degré premier est une fonction rationnelle de deux racines particulières quelconques, les coefficients de cette fonction faisant partie du domaine de rationalité.*

Nous allons démontrer la réciproque :

Si les racines d'une équation irréductible de degré premier sont fonctions rationnelles de deux d'entre elles, l'équation est résoluble algébriquement.

Soient

$$x_2 = \theta_2(x_0, x_1), \qquad x_3 = \theta_3(x_0, x_1), \qquad \ldots, \qquad x_{n-1} = \theta_{n-1}(x_0, x_1)$$

les expressions des racines $x_2, x_3, \ldots, x_{n-1}$ au moyen de x_0 et x_1, et

$$G = (S_1 = 1, \quad S_2, \quad S_3, \quad \ldots, \quad S_r)$$

le groupe de l'équation ; toute substitution de ce groupe laissant x_0 et x_1 fixes ne peut changer aucun autre élément ; on en conclut qu'il ne renferme pas deux substitutions distinctes amenant x_0 et x_1 à des places déterminées dans la suite $x_0, x_1, \ldots, x_{n-1}$. Supposons en effet que S_α et S_β soient deux substitutions remplaçant x_{i_0} et x_{i_1} par x_0 et x_1 ; le produit $S_\alpha S_\beta^{-1}$ laisse x_0 et x_1 fixes et se réduit à l'unité, de sorte que S_α et S_β ne peuvent être différentes.

Les substitutions de G, sauf l'unité, doivent changer au moins un des deux éléments x_0, x_1, et il y a $n(n-1)$ manières de placer ceux-ci ; si les substitutions S produisent tous les changements possibles de x_0 et x_1, on a $r = n(n-1)$; plus généralement, considérons le groupe G et le groupe formé des substitutions

$$\Sigma_1, \Sigma_2, \ldots, \Sigma_{(n-2)!}$$

laissant x_0 et x_1 invariables et permutant $x_2, x_3, \ldots, x_{n-1}$ de toutes les manières possibles. Formons un tableau analogue à celui du § 6, constitué par les lignes

$$S_1\Sigma_\alpha, S_2\Sigma_\alpha, \ldots, S_r\Sigma_\alpha \qquad [\alpha = 1, 2, \ldots, (n-2)!] ;$$

les substitutions qu'il renferme sont distinctes, car celles d'une même ligne le sont, et si l'on avait d'autre part

$$S_h\Sigma_\alpha = S_k\Sigma_\beta \qquad (h \neq k),$$

le produit $S_k^{-1}S_h = \Sigma_\beta\Sigma_\alpha^{-1}$ serait une substitution de G laissant x_0 et x_1 fixes et se réduirait à l'unité, ce qui est impossible.

D'autre part, ce tableau renferme toutes les substitutions amenant x_0 et x_1 aux places qu'ils occupent simultanément par l'effet des substitutions S, et $x_2, x_3, \ldots, x_{n-1}$ aux autres places dans un ordre quelconque ; par suite il est constitué par les substitutions d'un groupe dont l'ordre est égal à $r(n-2)!$. Comme cet ordre doit diviser $n!$ c'est-à-dire le produit $n(n-1)(n-2)!$, on voit que l'ordre r du groupe G est un diviseur de $n(n-1)$.

Ce groupe doit contenir, comme sous-groupe, au moins un groupe cyclique, d'après le théorème I ; je dis qu'il ne peut en contenir

deux. Supposons en effet qu'il contienne les deux groupes

$$C_1 = [S_1 = (x_0 x_1 x_2 \ldots x_{n-1}), \quad S_1^2, \ \ldots, \ S_1^n = 1],$$
$$C_2 = [T_1 = (x_0 x_1 x_{i_2} \ldots x_{i_{n-1}}), \quad T_1^2, \ \ldots, \ T_1^n = 1];$$

les substitutions $S_1^\alpha T_1^\beta$ sont toutes distinctes, car si l'on avait

$$S_1^\alpha T_1^\beta = S_1^\gamma T_1^\delta,$$

on aurait $T_1^{\beta-\delta} = S_1^{\gamma-\alpha}$ et, r étant choisi de façon que

$$r(\beta - \delta) \equiv 1 \qquad (\text{mod. } n),$$

on en déduirait

$$T_1 = S_1^{(\gamma-\alpha)r},$$

de sorte que T_1 ferait partie du groupe C_1, ce qui est impossible puisque ces groupes n'ont aucune substitution commune ; par suite le groupe G contenant C_1 et C_2 a un ordre au moins égal à n^2, et c'est impossible puisque cet ordre doit diviser $n(n-1)$.

On conclut de là, d'après ce que nous avons vu précédemment, que l'équation est résoluble algébriquement.

Une équation irréductible de degré premier dont les racines s'expriment rationnellement au moyen de deux d'entre elles s'appelle une équation de Galois (*). On peut dès lors énoncer les résultats que nous venons d'obtenir sous la forme suivante :

Théorème V. — *Pour qu'une équation irréductible de degré premier soit résoluble algébriquement, il faut et il suffit qu'elle soit une équation de Galois.*

102. Comme exemple de ce qui précède, l'équation binome générale de degré premier

$$f(x) = x^n - c_n(R', R'', \ldots) = 0,$$

telle que c_n ne soit pas la puissance n^e exacte d'une fonction du domaine de rationalité, est une équation de Galois.

Elle est d'abord irréductible, car sinon le théorème du § 65 montrerait que c_n est une puissance n^e exacte, contrairement à l'hypothèse ; de plus si ses racines sont

$$x_0, \qquad x_1 = \omega x_0, \qquad x_2 = \omega^2 x_0, \qquad \ldots, \qquad x_{n-1} = \omega^{n-1} x_0,$$

(*) Galois, *Œuvres mathématiques, Journal de Liouville*, 1846.

où ω est une racine n^e de l'unité, on a

$$x_k = x_0\left(\frac{x_1}{x_0}\right)^k,$$

de sorte que chaque racine est une fonction rationnelle de x_0 et x_1.

L'équation est donc résoluble au moyen de radicaux ; ses racines sont du reste le produit du radical $\sqrt[n]{c_n}$ par les racines n^{es} de l'unité qui sont elles-mêmes, comme on le sait, exprimables au moyen de radicaux.

Un autre exemple est fourni par l'équation qui donne $\operatorname{tg}\frac{a}{n}$ connaissant $\operatorname{tg} a$; elle a en effet pour racines les valeurs

$$x_0 = \operatorname{tg}\frac{a}{n}, \qquad x_1 = \operatorname{tg}\frac{a+\pi}{n}, \qquad x_2 = \operatorname{tg}\frac{a+2\pi}{n}, \qquad \ldots,$$

qui donnent lieu aux relations

$$\operatorname{tg}\frac{\pi}{n} = \frac{x_1 - x_0}{1 + x_1 x_0},$$

$$x_k = \frac{x_{k-1} + \operatorname{tg}\dfrac{\pi}{n}}{1 - x_{k-1}\operatorname{tg}\dfrac{\pi}{n}},$$

de sorte que x_k est fonction rationnelle de x_0 et x_1. Dans le cas de n premier, l'équation est irréductible et se résout par suite au moyen de radicaux.

Lorsque l'on adjoint $\operatorname{tg}\frac{\pi}{n}$ au domaine de rationalité, l'équation est abélienne, comme nous l'avons vu au § 82, car chaque racine est la même fonction rationnelle de la précédente.

103. Nous donnerons pour terminer l'expression des racines d'une équation irréductible et résoluble de degré premier.

Nous avons vu au § 87 que les racines $x_0, x_1, \ldots, x_{n-1}$ d'une équation de degré premier n s'expriment au moyen des fonctions

$$\psi_k = \sum_{r=0}^{n-1} \omega^{kr} x_r$$

par la formule

$$n x_l = \sum_{k=0}^{n-1} \omega^{-lk}\psi_k = \psi_0 + \sum_{k=1}^{n-1} \omega^{-lk}\psi_k ;$$

tout revient à calculer les fonctions ψ. Nous prendrons une racine primitive (mod. n) que nous désignerons par g, et nous supposerons que $g^{n-1}-1$ ne soit pas divisible par n^2; si nous posons $k=g^q$, q est appelé l'indice de k, ce que l'on écrit sous la forme $q=\text{ind}.\,k$.

Nous avons remarqué que les fonctions $\psi_{ht}\psi_t^{-h}$, que nous avons désignées par φ_h, sont des fonctions cycliques des racines; nous considérerons ici les fonctions analogues

$$y_q=\psi_{g^q}\psi_{g^{q-1}}^{-g} \qquad (q=1,2,\ldots,n-1);$$

ce sont des fonctions cycliques de $x_0, x_1, \ldots, x_{n-1}$ appartenant au même groupe, et s'exprimant rationnellement au moyen de l'une d'elles. Une fonction cyclique des $n-1$ quantités y est une fonction métacyclique des racines x, et par suite s'exprime rationnellement au moyen des coefficients de l'équation; on peut ajouter qu'elle est indépendante de la racine ω, car le changement de ω en ω^g transforme simplement y_i en y_{i+1}; par conséquent $y_1, y_2, \ldots, y_{n-1}$ sont les racines d'une équation abélienne de degré $n-1$ dont les coefficients sont rationnels et dépendent seulement de ceux de l'équation.

Si l'on forme le produit

$$\text{P}=y_a y_{a-1}^g y_{a-2}^{g^2}\ldots y_{a-n+2}^{g^{n-2}},$$

il se réduit à $\psi_{g^a}^{1-g^{n-1}}$; si l'on pose $\dfrac{1-g^{n-1}}{n}=-sn+g^b$, où les deux nombres s et b sont convenablement choisis, le second étant positif, le produit P est la n^e puissance de $\psi_{g^a}^{-sn+g^b}$. Comme on a

$$\psi_{g^{a+b}}=\psi_{g^a}^{g^b} y_{a+b} y_{a+b-1}^g \ldots y_{a+1}^{g^{b-1}},$$

il en résulte l'égalité suivante

$$\psi_{g^{a+b}}=\psi_{g^a}^{sn} y_{a+b} y_{a+b-1}^g \ldots y_{a+1}^{g^{b-1}} \text{P}^{\frac{1}{n}}.$$

Le facteur de $\text{P}^{\frac{1}{n}}$ au second membre est une fonction cyclique que l'on peut exprimer en fonction rationnelle de y_a; si on la représente par $\text{F}(y_a)$, il vient

$$\psi_{g^{a+b}}=\text{F}(y_a)\left[y_a y_{a-1}^g y_{a-2}^{g^2}\ldots y_{a-n+2}^{g^{n-2}}\right]^{\frac{1}{n}};$$

les indices et les exposants peuvent être réduits à leur plus petit reste positif (mod. n), en modifiant la fonction F.

Cette fonction est indépendante de ω, car le changement de ω en ω^g revient à augmenter a d'une unité ; comme la formule précédente est vraie quel que soit a, les coefficients de F ne peuvent être altérés par ce changement.

Nous avons ainsi déterminé les fonctions ψ ; remarquons toutefois que les quantités y, qui sont racines d'une équation abélienne de degré $n-1$, ne sont pas entièrement déterminées, et qu'on peut représenter par y_1 l'une quelconque d'entre elles, les autres étant déterminées par cela même ; nous pouvons donc sans inconvénient remplacer au second membre a par $a+b$ et poser $a+b=q=\text{ind.}\,k$. D'autre part un des facteurs du second membre tel que $y_{a-\alpha}^{g^\alpha}$ peut encore s'écrire $y^\beta{}_{\text{ind.}\,k-\text{ind.}\,\beta}$ ou $y^\beta{}_{\text{ind.}\,\frac{k}{\beta}}$, si $\beta \equiv g^\alpha \pmod{n}$; on peut donc écrire finalement

$$\psi_k = \text{F}(y_{\text{ind.}\,k}) \prod_{r=1}^{n-1} y_{\text{ind.}\,\frac{k}{r}}^{\frac{r}{n}}.$$

Telle est la formule donnée par Kronecker et reproduite dans l'*Algèbre supérieure* de Serret ; les quantités y sont les racines d'une équation abélienne de degré $n-1$ à coefficients rationnels et F est une fonction rationnelle.

On démontre que les racines déterminées au moyen des fonctions précédentes par la formule

$$nx_l = \sum_{k=0}^{n-1} \omega^{-lk}\psi_k$$

sont celles d'une équation résoluble de degré n quelle que soit la fonction F et l'équation abélienne dont $y_1, y_2, \ldots, y_{n-1}$ sont les racines.

Par exemple dans le cas de $n=5$, prenons pour racine primitive le nombre $g=2$; on a

$g^0 \equiv 1, \qquad g \equiv 2, \qquad g^2 \equiv 4, \qquad g^3 \equiv 3, \qquad g^4 \equiv 1 \pmod{5},$

de sorte que l'on obtient

$$\psi_1 = \text{F}(y_4) y_4^{\frac{1}{5}} y_3^{\frac{2}{5}} y_1^{\frac{3}{5}} y_2^{\frac{4}{5}},$$

et des expressions analogues pour ψ_2, ψ_3 et ψ_4 ; y_1, y_2, y_3 et y_4 ont les valeurs que nous avons déterminées au § 89 en cherchant les racines d'une équation abélienne du quatrième degré.

CHAPITRE XIII

DU GROUPE D'UNE ÉQUATION

---

104. Nous avons vu au § 45 que chaque équation est caractérisée par un groupe particulier de substitutions G satisfaisant aux conditions suivantes :

Toute fonction des racines numériquement invariable pour les substitutions du groupe s'exprime rationnellement au moyen des éléments du domaine de rationalité, et, réciproquement, toute fonction des racines s'exprimant rationnellement reste numériquement invariable pour les substitutions du groupe.

L'étude de ce groupe est le fondement des recherches de Galois sur les équations algébriques, et le *Traité des Substitutions* de M. Jordan, où elles sont exposées en même temps que celles de l'auteur, montre l'heureux parti que l'on peut tirer de la théorie des groupes dans les recherches algébriques ; nous n'exposerons pas ici tous les résultats donnés par M. Jordan, et nous renverrons à son œuvre magistrale ceux qu'intéressent ces questions difficiles ; nous ne pouvons cependant nous dispenser d'indiquer les principales applications de la théorie des groupes à l'étude des équations.

Nous avons démontré au § 48 le théorème suivant :

Théorème I. — *Toute équation irréductible a son groupe transitif, et réciproquement.*

Nous énoncerons encore la propriété suivante :

Théorème II. — *L'ordre d'un groupe transitif est un multiple de son degré.*

Considérons en effet les substitutions laissant un élément tel que x_1 invariable, et désignons-les par $S_1, S_2, \ldots, S_{r'}$; d'après la propriété du groupe d'être transitif, il existe au moins une substitution Σ_2 remplaçant x_1 par x_2, et de même des substitutions $\Sigma_3, \ldots, \Sigma_n$ remplaçant x_1 par $x_3, \ldots, x_n$. En représentant par Σ_1 la substitution unité, formons le tableau

$$\begin{array}{cccc} S_1\Sigma_1, & S_2\Sigma_1, & \ldots, & S_{r'}\Sigma_1 \\ S_1\Sigma_2, & S_2\Sigma_2, & \ldots, & S_{r'}\Sigma_2 \\ \ldots & \ldots & \ldots & \ldots \\ S_1\Sigma_n, & S_2\Sigma_n, & \ldots, & S_{r'}\Sigma_n \end{array}$$

analogue au tableau (4) du § 6 ; en répétant un raisonnement connu, on voit que les substitutions de la seconde ligne sont distinctes et distinctes des premières, remplacent x_1 par x_2, et que ce sont les seules jouissant de cette propriété ; de la même manière celles de la troisième ligne remplacent x_1 par x_3, et ainsi de suite. Ce tableau renferme toutes les substitutions du groupe donné, de sorte que l'ordre de ce groupe est égal à $r'n$; on voit qu'il est un multiple du degré n.

Si r' est égal à l'unité, il n'existe aucune substitution laissant un élément quelconque invariable, à part la substitution unité, et réciproquement ; on peut donc énoncer ce corollaire :

Corollaire. — *Un groupe transitif dont l'ordre est égal au degré ne renferme aucune substitution autre que l'unité laissant un élément invariable, et réciproquement ; il contient une et une seule substitution remplaçant un élément par un autre donné à l'avance arbitrairement.*

Un groupe cyclique composé d'une substitution circulaire et de ses puissances jouit de la propriété que nous venons d'énoncer. Un autre exemple nous est fourni par la considération de l'équation résolvante de Galois ; nous avons vu qu'à chaque groupe G d'ordre r relatif à une équation de degré n correspondent r valeurs $\psi_1, \psi_2, \ldots, \psi_r$ de la fonction de Galois, constituant les racines de l'équation résolvante (§ 45 et 46) ; à chaque substitution du groupe G effectuée sur les éléments $x_1, x_2, \ldots, x_n$ correspond une substitution effectuée sur les r éléments ψ ; les r substitutions ainsi formées sur ces derniers sont celles d'un groupe G' dont l'ordre est égal au degré, et jouissent des propriétés énoncées dans le corollaire précédent.

Les deux groupes G et G′ ont entre eux une dépendance mutuelle caractérisée par ce fait qu'à chaque substitution de l'un correspond une et une seule substitution de l'autre, et au produit de deux substitutions du premier correspond le produit des deux homologues du second et réciproquement. Deux tels groupes sont appelés *isomorphes* ; on peut donc dire que tout groupe transitif d'ordre r est isomorphe à un groupe de même ordre, dont l'ordre et le degré sont égaux.

105. Une propriété des groupes transitifs est la primitivité ou la non-primitivité. On dit qu'un groupe transitif G est *non-primitif* si l'on peut ranger les éléments $x_1, x_2, \ldots, x_n$ en plusieurs séries d'un même nombre de lettres

$$(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_\mu}), (x_{\beta_1}, x_{\beta_2}, \ldots, x_{\beta_\mu}), \ldots$$

telles que chaque substitution du groupe permute entre elles les lettres de chaque série ou les remplace toutes par celles d'une autre série ; le groupe sera dit *primitif* s'il n'est pas possible de grouper les éléments de cette façon.

Un groupe de degré premier est primitif ; un groupe cyclique de degré composé n, formé par les puissances d'une substitution circulaire d'ordre n est non-primitif ; soit par exemple pour six éléments le groupe cyclique

$$G = [1, (x_1x_2x_3x_4x_5x_6), (x_1x_3x_5)(x_2x_4x_6), (x_1x_4)(x_2x_5)(x_3x_6), (x_1x_5x_3)(x_2x_4x_6), (x_1x_6x_5x_4x_3x_2)];$$

on peut prendre les deux systèmes $(x_1, x_3, x_5), (x_2, x_4, x_6)$ ou bien encore les trois systèmes $(x_1, x_4), (x_2, x_5), (x_3, x_6)$; ils jouissent de la propriété énoncée relativement aux substitutions du groupe G.

Les substitutions d'un groupe non primitif peuvent être mises sous forme d'un tableau de la manière suivante : Composons une première ligne au moyen des substitutions qui laissent les éléments de chaque série invariables, ou les permutent entre eux, mais non avec ceux d'une autre série ; soient

$$S_1, \quad S_2, \quad \ldots, \quad S_{r'}$$

ces substitutions. Soit maintenant Σ_2 une substitution changeant au moins un élément d'une série dans un autre d'une autre série ; les produits

$$S_1\Sigma_2, \qquad S_2\Sigma_2, \qquad \ldots, \qquad S_{r'}\Sigma_2$$

sont distincts l'un de l'autre et des premières substitutions ; ils formeront une deuxième ligne ; si toutes les substitutions ne sont pas épuisées, on prendra une nouvelle substitution Σ_3, et les produits de $S_1, S_2, \ldots, S_{r'}$ par Σ_3, et ainsi de suite ; en répétant un raisonnement connu, on peut mettre toutes les substitutions sous forme d'un tableau identique au tableau (4) du § 6 ; l'ordre r du groupe est égal à $r'\rho$.

On peut ajouter que le groupe

$$G_1 = (S_1 S_2 \ldots S_{r'})$$

est un sous-groupe invariant de G, de sorte que tout groupe non primitif est en même temps composé. De la même manière, les groupes $H_1, H_2, \ldots$ formés des substitutions qui ne changent que les éléments de chacune des séries successives, en laissant invariables ceux des autres, sont des sous-groupes invariants de G et de G_1 et sont semblables.

106. Théorème III. — *L'équation de degré $m_1 m_2$ que l'on obtient en éliminant y entre deux équations irréductibles,*

$$(1) \qquad \varphi_2(y) = y^{m_2} + a_1 y^{m_2-1} + \cdots + a_{m_2} = 0,$$

$$(2) \qquad \varphi_1(x, y) = x^{m_1} + b_1(y) x^{m_1-1} + \cdots + b_{m_1}(y) = 0,$$

a un groupe non primitif, et, réciproquement, toute équation de groupe non primitif est le résultat d'une semblable élimination.

Soit, en effet, y_α une des racines de l'équation (1) ; l'équation à laquelle satisfait x est

$$(3) \qquad f(x) = \Pi_\alpha \varphi_1(x, y_\alpha) = 0.$$

Soient $x_{\alpha 1}, x_{\alpha 2}, \ldots, x_{\alpha m_1}$ les racines de $\varphi_1(x, y_\alpha) = 0$; toute fonction symétrique F_α de ces racines est rationnellement exprimable au moyen de y_α et toute fonction symétrique de $F_1, F_2, \ldots, F_\alpha, \ldots, F_{m_2}$ est rationnelle dans le domaine des coefficients de l'équation (1) ; par suite toute fonction des racines restant invariable quand on effectue les substitutions qui changent entre elles les racines de chacune des séries

$$(4) \qquad x_{\alpha 1}, x_{\alpha 2}, \ldots, x_{\alpha m_1} \qquad (\alpha = 1, 2, \ldots, m_2)$$

ou les permutent avec celles d'une autre série, et cela de toutes les manières possibles, est rationnellement exprimable ; le groupe composé de ces substitutions n'est pas primitif ; comme les fonctions

des racines qui lui appartiennent sont des fonctions rationnelles des coefficients de l'équation, il est identique au groupe de l'équation (3) ou le contient comme sous-groupe ; dès lors ce dernier jouit de la même propriété.

Réciproquement, soit G un groupe non primitif relatif à une équation irréductible, et soient (4) les m_2 séries de m_1 éléments qui entrent dans les substitutions du groupe ; considérons les fonctions symétriques des racines de chaque série

$$y_\alpha = F_\alpha(x_{\alpha 1}, x_{\alpha 2}, \ldots, x_{\alpha m_1})\,;$$

elles restent invariables ou se permutent les unes dans les autres par les substitutions de G ; par suite le produit

$$\varphi_2(y) = (y - y_1)(y - y_2)\ldots(y - y_{m_2})$$

est invariable pour le groupe G et a ses coefficients rationnels dans le domaine. Lorsqu'on a déterminé une racine y_α, on peut calculer toutes les fonctions symétriques des racines $x_{\alpha 1}, x_{\alpha 2}, \ldots$ et former l'équation

$$\varphi_1(x, y_\alpha) = 0$$

dont elles dépendent. Comme on a

$$f(x) = \Pi_\alpha \varphi_1(x, y_\alpha),$$

l'équation donnée résulte de l'élimination de y entre deux équations de la forme (1) et (2).

Nous avons rencontré un exemple d'une équation dont le groupe n'est pas primitif lorsque nous avons résolu l'équation abélienne simple de degré composé n. Le groupe de cette équation est formé de la substitution circulaire d'ordre n et de ses puissances ; il n'est pas primitif, et si $n = m_1 m_2$, la résolution de l'équation se fait au moyen de deux équations successives de degrés m_1 et m_2. Le groupe d'une équation abélienne quelconque de degré composé jouit de la même propriété.

107. Considérons une équation de groupe G, $\varphi(x_1, x_2, \ldots, x_n)$ une fonction des racines appartenant au groupe, et $\varphi_1(x_1, x_2, \ldots, x_n)$ une autre fonction quelconque des racines appartenant numériquement à un groupe G_1, ; lorsqu'on adjoint cette deuxième fonction au domaine de rationalité, c'est la fonction $u\varphi + u_1\varphi_1$ qui est rationnellement exprimable dans le nouveau domaine, et toute autre jouissant de cette propriété peut être exprimée rationnellement au

moyen de $u\varphi + u_1\varphi_1$ et des coefficients ; il en résulte que le groupe de l'équation est celui de cette dernière fonction, et il se compose des substitutions communes aux groupes G et G_1. Plus généralement, l'adjonction de plusieurs fonctions des racines au domaine de rationalité réduit le groupe de l'équation aux substitutions communes au groupe primitif et à ceux auxquels appartiennent les fonctions adjointes.

On voit de cette façon quel effet produit sur une équation l'adjonction de racines d'équations résolvantes successives ; l'équation reste irréductible ou se réduit suivant que le nouveau groupe est transitif ou non. Le problème de la résolution d'une équation générale ou spéciale peut alors être envisagé de la manière suivante : Chercher des fonctions des racines fournies par des équations résolvantes, dont l'adjonction réduise peu à peu le groupe de l'équation à la substitution unité ; lorsque ce résultat est atteint, l'équation est résolue, car la fonction de Galois dont le groupe est constitué par cette seule substitution est déterminée, et l'on en déduit les racines elles-mêmes.

C'est précisément la marche que nous avons suivie dans la résolution des équations du troisième et du quatrième degré par la méthode de Lagrange.

Dans le cas de l'équation du troisième degré générale, ayant pour groupe le groupe symétrique, l'adjonction d'une fonction alternée ou de la racine carrée du discriminant le réduit au groupe alterné ; celle de la racine cubique d'une fonction alternée particulière le réduit ensuite à l'unité, et l'équation est résolue.

En ce qui concerne l'équation du quatrième degré, de groupe G (§ 54), l'adjonction d'une racine φ_1 de l'équation résolvante de Lagrange le réduit au groupe G_1 ; celle d'une racine t_1 de l'équation

$$t^2 - \varphi_1 t + c_1 = 0$$

le réduit ensuite au groupe g_1. Ce dernier groupe n'est pas transitif et l'équation se décompose dans le nouveau domaine de rationalité, en deux autres ayant pour racines l'une x_1 et x_2, l'autre x_3 et x_4.

Lorsque le groupe d'une équation n'est pas primitif, comme celui que nous avons considéré au § précédent, l'adjonction de la racine y_α de l'équation $\varphi_2(y) = 0$ le réduit au groupe dont les substitutions permutent entre eux les m_1 éléments

$$x_{\alpha 1},\ x_{\alpha 2},\ \ldots,\ x_{\alpha m_1},$$

ou bien les $m_1(m_2 - 1)$ autres, mais non les premiers avec ceux-ci ; ce dernier groupe n'est pas transitif et l'équation est réductible, l'un des facteurs du premier membre étant $\varphi_1(x, y_\alpha)$.

Nous indiquerons une application importante des considérations qui précèdent.

Théorème IV. — *Si une équation irréductible jouit de la propriété que toutes ses racines s'expriment rationnellement au moyen de l'une d'elles, elle a un groupe transitif dont l'ordre est égal au degré, et réciproquement.*

Soient en effet $x_1, x_2, \ldots, x_n$ les racines d'une équation irréductible de degré n ; supposons qu'elles s'expriment rationnellement au moyen de l'une d'elles x_1, et que l'on ait

$$x_2 = \theta_2(x_1), \qquad x_3 = \theta_3(x_1), \qquad \ldots, \qquad x_n = \theta_n(x_1)\ ;$$

le groupe de cette équation est transitif, puisque l'équation est irréductible ; ses substitutions ne doivent pas changer les relations précédentes, par suite celles qui laissent x_1 invariable ne peuvent altérer $x_2, x_3, \ldots, x_n$. Il n'existe que la substitution unité jouissant de cette propriété ; dès lors, d'après les raisonnements que nous avons faits au § 104, l'ordre du groupe est égal à son degré.

Réciproquement, supposons que le groupe d'une équation de degré n soit transitif et ait son ordre égal à son degré ; cette équation est d'abord irréductible ; de plus, si l'on adjoint au domaine de rationalité une racine quelconque telle que x_1, son groupe se réduit à celles de ses substitutions laissant x_1 invariable, c'est-à-dire à la substitution unité ; après cette adjonction, la fonction de Galois est rationnellement exprimable, et les racines de l'équation sont toutes des fonctions rationnelles de x_1.

Ce raisonnement nous montre de plus que *si les racines d'une équation irréductible sont des fonctions rationnelles de l'une d'entre elles, elles s'expriment aussi rationnellement au moyen de l'une quelconque des autres.*

L'équation résolvante de Galois et les équations abéliennes nous donnent des exemples des considérations précédentes.

108. Le groupe d'une équation abélienne générale irréductible est un groupe cyclique simple ou à plusieurs entrées ; il est transitif,

a son ordre égal à son degré, et de plus ses substitutions sont échangeables, c'est-à-dire que deux quelconques d'entre elles S_α et S_β sont telles que l'on ait $S_\alpha S_\beta = S_\beta S_\alpha$. Celui d'une équation abélienne quelconque, irréductible ou non, telle que nous l'avons définie au § 83, jouit aussi de la propriété d'avoir ses substitutions permutables ; nous allons démontrer la réciproque.

Théorème V. — *Toute équation dont le groupe est formé de substitutions échangeables est une équation abélienne.*

Pour cette raison, nous désignerons un tel groupe sous le nom de *groupe abélien*.

S'il n'est pas transitif, et si l'on décompose le premier membre de l'équation en facteurs irréductibles, les groupes des équations partielles obtenues sont formés d'une partie des substitutions du groupe total et sont encore abéliens ; il nous suffit donc de nous limiter aux groupes transitifs.

Reprenons le tableau du § 104 et désignons par S_α une substitution quelconque laissant x_1 invariable ; pour que cette substitution soit échangeable avec Σ_2, c'est-à-dire que l'on ait $S_\alpha\Sigma_2 = \Sigma_2 S_\alpha$, il est nécessaire qu'elle n'altère pas l'élément x_2, comme on le voit immédiatement ; pour la même raison, S_α ne peut être permutable avec $\Sigma_3, \ldots, \Sigma_n$ que si elle laisse invariables $x_3, \ldots, x_n$, c'est-à-dire si elle se réduit à l'unité ; de cette façon r' est égal à l'unité, et le groupe a son ordre égal à son degré. D'après le théorème IV, toutes les racines de l'équation sont fonctions rationnelles de l'une d'elles, et l'on a par exemple

$$x_2 = \theta_2(x_1), \qquad x_3 = \theta_3(x_1), \qquad \ldots, \qquad x_n = \theta_n(x_1).$$

Si les substitutions Σ_α et Σ_β remplaçant x_1 par x_α et x_β sont échangeables, il en est de même des fonctions θ_α et θ_β ; on déduit de là que toutes les fonctions θ sont permutables, et que l'équation est abélienne, ce que nous voulions démontrer.

Les raisonnements que nous avons faits aux § 84 et 85 nous montrent qu'un groupe abélien est, pour une notation particulière des éléments, un groupe cyclique à une ou plusieurs entrées. Nous pouvons du reste étudier directement un groupe dont les substitutions sont échangeables par la méthode qui nous a servi à réduire les fonctions θ au nombre minimum d'éléments ; les raisonnements sont les mêmes, et nous pouvons énoncer ce résultat :

THÉORÈME VI. — *Si les substitutions d'un groupe transitif sont toutes permutables, il existe un système fondamental de substitutions* $S_1, S_2, \ldots, S_\nu$ *d'ordres respectifs* $n_1, n_2, \ldots, n_\nu$, *telles que les expressions*

$$S_1^{h_1}S_2^{h_2}\ldots S_\nu^{h_\nu} \qquad \begin{pmatrix} h_\alpha = 1, 2, \ldots, n_\alpha - 1 \\ \alpha = 1, 2, \ldots, \nu \end{pmatrix}$$

représentent une fois et une seule toutes les substitutions du groupe; chacun des nombres $n_1, n_2, \ldots, n_\nu$ *est divisible par le suivant ou lui est égal; l'ordre et le degré du groupe sont égaux au produit* $n_1 n_2 \ldots n_\nu$.

109. Nous avons supposé jusqu'à présent qu'on adjoint au domaine de rationalité une racine d'une équation résolvante, c'est-à-dire une fonction des racines $x_1, x_2, \ldots, x_n$ de l'équation donnée. Nous allons considérer le cas où l'on effectue l'adjonction d'une racine R_1 d'une équation $\varphi(R, R', R'', \ldots) = 0$ irréductible dans le domaine de rationalité primitif; on peut toujours, comme nous l'avons vu, ramener à ce cas celui où l'on adjoindrait plusieurs racines analogues.

Formons l'équation résolvante de Galois $\Psi_1(z) = 0$ dont le premier membre est irréductible et a un degré égal à l'ordre r du groupe G de l'équation donnée $f(x) = 0$, et adjoignons R_1 au domaine; si Ψ_1 se décompose en un produit de plusieurs facteurs, et si $\Psi_2(z)$ est celui qui renferme $z - \psi_1$, le groupe se réduit aux substitutions déterminées par ce facteur, constituant un sous-groupe G'_1 du premier.

On peut opérer une réduction identique du groupe G par l'adjonction d'une racine d'une équation résolvante particulière; prenons en effet une fonction $\varphi_1(x_1, x_2, \ldots, x_n)$ des racines de $f(x) = 0$ appartenant au groupe G'_1, et ses valeurs $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ pour les substitutions de G; ce sont les racines d'une équation irréductible

$$\Phi(z) = (z - \varphi_1)(z - \varphi_2)\ldots(z - \varphi_\rho) = 0$$

à coefficients rationnels dans le domaine primitif; l'adjonction de la racine φ_1 de cette équation produit sur le groupe G le même effet que celle de R_1.

Nous pouvons aller plus loin et montrer que l'adjonction des différentes racines de $\varphi(R, R', R'', \ldots) = 0$, que nous désignerons

par $R_1, R_2, \ldots, R_\nu$, peut être remplacée par celle des racines de $\Phi(z) = 0$.

Remarquons d'abord que φ_1 est une fonction appartenant au groupe G'_1 de l'équation et par suite est rationnellement exprimable au moyen de R_1 ; soit par exemple $\varphi_1 = \theta(R_1)$ sa valeur ; l'équation

$$[\theta(z) - \varphi_1][\theta(z) - \varphi_2]\ldots[\theta(z) - \varphi_\rho] = 0$$

a avec $\varphi(R) = 0$ la racine commune R_1, par suite elle est satisfaite pour les autres racines $R_2, \ldots, R_\nu$, et chacune des expressions $\theta(R_i)$ est égale à l'une des quantités φ. On conclut de là que le polynome

$$F(z) = [z - \theta(R_1)][z - \theta(R_2)]\ldots[z - \theta(R_\nu)],$$

qui s'annule pour certaines des valeurs $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ et pour aucune autre, est une puissance exacte de $\Phi(z)$, et que l'on a par exemple $F(z) = \Phi(z)^\mu$; dès lors μ des valeurs $\theta(R_i)$ sont égales à φ_1, μ autres à φ_2, etc.

Cela posé, admettons que l'on ait $\theta(R_\alpha) = \varphi_\alpha$, et désignons par G'_α et G''_α les groupes auxquels se réduit celui de l'équation lorsqu'on adjoint respectivement R_α et φ_α ; d'après ce que nous avons vu au § 39, R_1 et R_α produisent des décompositions analogues de l'équation résolvante $\Psi_1(z) = 0$ et les groupes G'_α et G'_1 ont le même ordre ; il en est de même de G''_α et de G'_1 ; comme φ_α est rationnellement exprimable après adjonction de R_α, le groupe G'_α contient toutes les substitutions de G''_α, et ces deux groupes sont identiques.

Il est donc indifférent d'adjoindre les racines de $\varphi(R) = 0$ ou celles de l'équation résolvante $\Phi(z) = 0$; nous nous placerons désormais dans le cas où les quantités introduites dans le domaine de rationalité sont des fonctions des racines de l'équation.

110. Considérons en particulier le cas où le degré n de l'équation donnée $f(x) = 0$ est un nombre premier ; si le groupe G se réduit, après l'adjonction de la fonction φ_1, à un groupe G'_1 non transitif, l'équation ne reste pas irréductible ; désignons par $f_1(x, \varphi_1)$ un des facteurs irréductibles de $f(x)$ dans le nouveau domaine, et par n' le degré de ce facteur.

Le produit

$$F(x) = f_1(x, \varphi_1)f_1(x, \varphi_2)\ldots f_1(x, \varphi_\rho),$$

étendu à toutes les racines de l'équation $\Phi(z) = 0$, s'annule pour

une au moins des racines de $f(x) = 0$; par suite il est divisible par le premier membre de l'équation donnée, et se décompose généralement, dans le domaine primitif, en plusieurs facteurs irréductibles dont l'un est égal à $f(x)$. Par un raisonnement analogue à celui que nous avons fait au § 98, nous voyons que ces facteurs se transforment les uns dans les autres par les substitutions du groupe G, et sont identiques; nous en concluons que l'on a par exemple $F(x) = f(x)^\lambda$.

De là résulte que le degré $n'\rho$ de $F(x)$ est égal à λn; comme n est un nombre premier supérieur à n', ρ doit être égal à n ou à un de ses multiples. Nous avons vu d'autre part que le degré ν d'une équation irréductible telle que $\varphi(R) = 0$, dont la racine R_1 produit la même réduction du groupe G que φ_1, est lui-même de la forme $\mu\rho$; il est donc aussi un multiple de n, et l'on peut énoncer ce résultat :

Théorème VII. — *Si une équation irréductible de degré premier n devient réductible après adjonction au domaine de rationalité d'une racine d'une équation $\varphi(R) = 0$ irréductible dans ce domaine, le degré de cette dernière est égal à n ou à un de ses multiples.*

Une conséquence importante de ce théorème peut être énoncée relativement à l'équation binome irréductible

$$x^n - F(R', R'', \ldots) = 0$$

de degré premier; elle reste irréductible par l'adjonction au domaine de rationalité d'une racine d'une équation quelconque de degré inférieur à n, en particulier par l'adjonction d'une racine n^e de l'unité ω_n, car cette dernière satisfait à une équation de degré $n-1$. Cette remarque peut être appliquée aux équations binomes de la chaîne dont il est question au § 64.

111. Le cas le plus important est celui où l'on adjoint à la fois toutes les racines d'une équation résolvante irréductible dans le domaine de rationalité primitif; soit φ une fonction du groupe G de l'équation $f(x) = 0$, dont les racines sont $x_1, x_2, \ldots, x_n$,

$$\Phi(z) = (z - \varphi_1)(z - \varphi_2)\ldots(z - \varphi_m) = 0$$

une équation ayant pour racines les valeurs distinctes d'une fonction $\varphi_1(x_1, x_2, \ldots, x_n)$ pour les substitutions de G, et soient $G_1, G_2, \ldots, G_m$ les groupes de ces fonctions; nous avons vu que

l'adjonction simultanée de $\varphi_1, \varphi_2, \ldots, \varphi_m$ réduit le groupe au sous-groupe H commun à $G, G_1, G_2, \ldots, G_m$.

C'est un sous-groupe invariant de G, car si l'on effectue sur les valeurs $\varphi_1, \varphi_2, \ldots, \varphi_m$ les substitutions du groupe de l'équation, elles se reproduisent à l'ordre près, et les groupes $G_1, G_2, \ldots, G_m$ sont des transformés de l'un d'entre eux par G ; dès lors le groupe H qui leur est commun est permutable à toute substitution de celui de l'équation et en est un sous-groupe invariant.

Considérons par exemple l'équation générale du quatrième degré, et l'équation résolvante dont les racines, deux à deux égales et de signes contraires, sont les six valeurs de

$$\chi_1 = x_1 + x_2 - x_3 - x_4 ;$$

elles appartiennent aux groupes g_1, g_2, g_3 n'ayant d'autre substitution commune que l'unité, et leur adjonction simultanée réduit le groupe de l'équation à la substitution identique, de sorte que l'équation se trouve résolue ; c'est ce que nous avons constaté au § 56.

De la même manière, l'adjonction simultanée des trois racines $\varphi_1, \varphi_2, \varphi_3$ de l'équation résolvante de Lagrange, appartenant respectivement aux groupes G_1, G_2, G_3, réduit le groupe de l'équation au groupe H qui leur est commun, et permet de calculer la fonction z_1 appartenant à ce groupe, ainsi que nous l'avons expliqué au § 58.

Supposons que le groupe G d'une équation soit simple ; le seul sous-groupe invariant qu'il possède est constitué par la substitution unité, et il se réduit à cette seule substitution par l'adjonction de toutes les racines d'une équation résolvante telle que $\Phi(z) = 0$; l'équation se trouve ainsi résolue. Au contraire, si le groupe G est composé et possède un sous-groupe invariant H, on peut former une fonction des racines le réduisant précisément à ce groupe H ; il suffit en effet de prendre une fonction appartenant à ce dernier groupe ; ses valeurs conjuguées pour les substitutions de G appartiennent au même groupe qui n'est autre que H lui-même (§ 22), de sorte qu'elles sont rationnellement exprimables au moyen de l'une d'elles ; l'adjonction d'une seule racine de l'équation résolvante dont dépendent ces valeurs conjuguées équivaut à celle de toutes les racines, et réduit le groupe de l'équation précisément au sous-groupe invariant H considéré. On peut ajouter que le degré de

l'équation résolvante est égal au quotient des ordres de G et de H.

En prenant pour H le sous-groupe invariant maximum de G, puis opérant sur ce nouveau groupe comme nous venons de l'indiquer, et ainsi de suite, on arrive au théorème suivant :

THÉORÈME VIII. — *Si une équation a un groupe* G *composé, si*

$$G, G_1, \ldots, G_\mu, 1$$

est une suite de composition de ce groupe, $e_1, e_2, \ldots, e_\mu, e_{\mu+1}$ *les facteurs de composition correspondants, on peut la résoudre au moyen d'équations successives de degrés* $e_1, e_2, \ldots, e_\mu, e_{\mu+1}$ *jouissant de la propriété d'être chacune irréductible dans le domaine auquel on adjoint les racines des équations précédentes, et d'avoir ses racines exprimées rationnellement, dans ce nouveau domaine, au moyen de l'une d'elles. Le groupe de l'équation se réduit, après adjonction successive d'une racine de chacune de ces équations, aux groupes*

$$G_1, G_2, \ldots, 1.$$

112. Nous allons appliquer ce théorème à l'étude des équations résolubles algébriquement. Si une équation donnée jouit de cette propriété, il existe, comme nous l'avons vu au chapitre IX, une chaîne d'équations binomes dont chacune est de degré premier et dont les racines sont des fonctions rationnelles des racines de l'équation proposée. Chacune d'elles est irréductible dans le domaine auquel on adjoint les irrationnelles déterminées précédemment et ses racines sont, dans ce nouveau domaine, exprimables rationnellement au moyen de l'une d'entre elles. On voit que l'adjonction des irrationnelles successives réduit progressivement le groupe G de l'équation à une série de groupes

$$G, \quad G_1, \quad G_2, \quad \ldots, \quad G_\mu, \quad 1$$

constituant une suite de composition de G, les facteurs de composition étant précisément les degrés $p_\nu, p_{\nu-1}, \ldots, p_1$ des équations binomes. Le groupe G doit donc être un groupe composé, les facteurs de composition étant premiers.

Cette condition, qui est nécessaire, est aussi suffisante ; supposons en effet qu'elle soit remplie, c'est-à-dire que les facteurs de composition du groupe de l'équation soient des nombres premiers ; supposons de plus que l'on soit déjà parvenu à réduire ce groupe

à un sous-groupe G_h de la suite de composition par l'adjonction d'une fonction rationnelle des racines déterminée au moyen d'une ou de plusieurs équations résolvantes. Si G_{h+1} est le groupe suivant, et si p_k est le nombre premier égal au rapport des ordres de G_h et G_{h+1}, il est possible, d'après le théorème du § 23, de former une fonction des racines appartenant au dernier de ces deux groupes, et ayant pour celles du premier p_k valeurs conjuguées racines d'une équation binome dont les coefficients font partie du groupe G_h; l'adjonction d'une de ces valeurs, c'est-à-dire d'un radical d'indice p_k, réduira le groupe à G_{h+1}. En opérant de cette manière à partir de G_1, il sera possible de former une chaîne d'équations binomes successives conduisant à la résolution algébrique de l'équation.

On peut par suite énoncer le théorème suivant :

THÉORÈME IX. — *La condition nécessaire et suffisante pour qu'une équation soit résoluble algébriquement est que les facteurs de composition de son groupe soient des nombres premiers.*

Les équations générales du troisième et du quatrième degré satisfont à la condition précédente. Le groupe de la première a pour facteurs de composition les nombres premiers 2 et 3, et nous avons constaté que sa résolution dépend de celle de deux équations binomes dont les degrés sont les nombres précédents. L'équation du quatrième degré a un groupe composé dont les facteurs de composition sont 2, 3, 2 et 2, et l'on a précisément, pour déterminer les racines de cette équation, à former des radicaux successifs dont ces nombres sont les indices.

Le groupe symétrique de n éléments, dans le cas où n est supérieur à 4, a pour facteurs de composition les deux nombres 2 et $\frac{n!}{2}$; comme le dernier n'est pas un nombre premier, l'équation générale de degré n n'est pas résoluble. Nous retrouvons ainsi le théorème d'Abel :

THÉORÈME X. — *L'équation générale de degré supérieur à quatre n'est pas résoluble algébriquement.*

NOTE D'ARITHMÉTIQUE

On dit qu'un nombre a est congru à un nombre b (module n) si la différence de ces deux nombres est un multiple de n ; on écrit ce fait de la manière suivante :

$$a \equiv b \pmod{n}.$$

Les congruences jouissent de la plupart des propriétés des égalités ; on peut additionner, soustraire, multiplier membre à membre des congruences de même module; dans le cas d'un module premier, l'analogie est plus complète, et l'on peut diviser membre à membre deux congruences de module premier si les termes de la seconde ne sont pas congrus à zéro.

Cela tient à ce que la congruence

$$ab \equiv 0 \pmod{n}$$

entraîne, pour n premier, l'une des deux congruences

$$a \equiv 0, \qquad b \equiv 0.$$

Si l'on considère alors les deux congruences

$$aa' \equiv bb' \pmod{n},$$

$$a \equiv b \pmod{n},$$

on a

$$a = b + mn,$$

$$(b + mn)a' - bb' = m'n,$$

$$b(a' - b') \equiv 0,$$

d'où l'on tire

$$a' \equiv b' \pmod{n};$$

cette dernière relation est donc une conséquence des deux premières.

Une congruence

$$ax + b \equiv 0 \pmod{n}$$

a toujours, pour n premier, une racine comprise entre 0 et n, lorsque a n'est pas $\equiv 0$, car sa recherche revient à la résolution de l'équation indéterminée

$$ax + ny + b = 0$$

en nombres entiers, et il existe toujours un nombre entier x, compris entre 0 et n, satisfaisant à cette équation.

La congruence suivante, où p est premier,

$$x^{p-1} \equiv 1 \pmod{p},$$

est satisfaite, d'après le théorème de Fermat, par tous les nombres $1, 2, \ldots, p-1$; soit a un nombre quelconque de cette suite ; formons la série des valeurs

$$1, a, a^2, a^3, \ldots, a^d, \ldots, a^{p-1}, \ldots,$$

et supposons que a^{m+d} soit le premier nombre congru à l'un des précédents (mod. p), par exemple à a^m ; on a

$$a^{m+d} \equiv a^m,$$

d'où l'on tire, en divisant par a^m les deux membres,

$$a^d \equiv 1 \pmod{p};$$

on en conclut que m doit être égal à zéro. Si d est le plus petit exposant satisfaisant à cette condition, il est un diviseur de $p-1$, car les nombres de la suite précédente se reproduisent de d en d, aux multiples près de p, et l'on doit avoir $a^{p-1} \equiv 1$; on dit que le nombre a appartient à l'exposant d.

Tout nombre qui appartient à l'exposant $p-1$ est dit une racine primitive (mod. p).

L'existence de racines primitives est fondée sur les considérations suivantes :

On sait que le nombre $\varphi(n)$ des nombres premiers avec n et inférieurs à lui, y compris l'unité, est donné par

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots,$$

si $n = p_1^{\alpha_1} p_2^{\alpha_2}\ldots$ est la décomposition du nombre donné en facteurs premiers ; $\varphi(n)$ est la fonction de Gauss ; je vais montrer que si d est un diviseur de $p-1$, il y a précisément $\varphi(d)$ nombres distincts suivant le module p, et appartenant à l'exposant d.

Désignons par $\psi(d)$ le nombre inconnu des nombres compris dans la suite $1, 2, \ldots, p-1$ appartenant à l'exposant d ; il peut être nul ; si nous nous plaçons dans le cas où il ne l'est pas, il y a un nombre a au moins tel que l'on ait $a^d \equiv 1$ et que les restes (mod. p) des nombres

$$1, a, a^2, \ldots, a^{d-1}$$

soient différents ; chacun d'eux satisfait à la congruence

$$x^d \equiv 1 \qquad \pmod{p},$$

de sorte que l'on a

$$x^d - 1 \equiv (x-1)(x-a)\ldots(x-a^{d-1}) \qquad \pmod{p}.$$

Il n'existe par suite aucun autre nombre que les précédents pouvant appartenir à d, mais ils ne lui appartiennent pas tous nécessairement ; prenons par exemple une puissance de a telle que a^h, où $h \leqq d-1$; si h est premier avec d, il n'existe aucun nombre de la suite

$$1, (a^h), (a^h)^2, \ldots, (a^h)^{d-1}$$

qui soit congru à l'un des autres (mod. n) ; si au contraire h n'est pas pre-

mier avec d, et si θ est le plus grand commun diviseur de ces deux nombres, on aura sûrement

$$(a^h)^{\frac{d}{\theta}} \equiv 1 \qquad (\text{mod. } p),$$

de sorte que a^h appartiendra à l'exposant $\frac{d}{\theta}$.

De cette façon le nombre des termes de la suite $1, a, \ldots, a^{d-1}$ appartenant à l'exposant d est égal à celui des nombres h premiers avec d et inférieur à lui, c'est-à-dire à $\varphi(d)$; le nombre $\psi(d)$ est par suite égal à zéro ou à $\varphi(d)$.

Si l'on prend tous les diviseurs $d, d', d'', \ldots$ de $p-1$, on a

$$\Sigma\psi(d) = p - 1\,;$$

d'autre part la somme des valeurs de $\varphi(d)$ est aussi égale à $p-1$; en effet si l'on a $p - 1 = p_1^{\alpha_1} p_2^{\alpha_2}\ldots$ et si $d = p_1^{\beta_1} p_2^{\beta_2}\ldots$ est un diviseur de ce nombre, on a

$$\varphi(d) = \varphi(p_1^{\beta_1})\varphi(p_2^{\beta_2})\ldots,$$

de sorte que $\Sigma\varphi(d)$ est le produit des polynomes

$$1 + \varphi(p_1) + \varphi(p_1^2) + \cdots,$$
$$1 + \varphi(p_2) + \varphi(p_2^2) + \cdots,$$
$$\ldots\ldots\ldots\ldots,$$

qui ont respectivement pour valeur $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots$; on a donc

$$\Sigma\varphi(d) = p - 1.$$

L'égalité

$$\Sigma\psi(d) = \Sigma\varphi(d)$$

entraîne alors l'égalité de chacun des nombres correspondants $\psi(d)$ et $\varphi(d)$, et l'on voit qu'il y a $\varphi(d)$ nombres appartenant à l'exposant d.

En particulier, il y a $\varphi(p-1)$ nombres appartenant à l'exposant $p-1$, c'est-à-dire qu'il y a $\varphi(p-1)$ racines primitives (mod. p).

TABLE DES MATIÈRES

Chapitre IV : **Relations algébriques entre les fonctions rationnelles de plusieurs variables.**

Chapitre V : **Des fonctions cycliques et métacycliques de plusieurs variables.**

Chapitre VI : **Domaine de rationalité. — Réductibilité des fonctions entières.**

Chapitre VII : **Des fonctions rationnelles des racines d'une équation. — Résolvantes. — Groupe d'une équation algébrique.**

Chapitre VIII : **Des équations du deuxième, du troisième et du quatrième degré. — Recherches de Lagrange.**

Chapitre IX : **De la résolution algébrique des équations.**

Chapitre X : **Des équations abéliennes.**

Chapitre XI : **Des équations de la division du cercle.**

Chapitre XII : **Des équations résolubles irréductibles de degré premier.**

Chapitre XIII : **Du groupe d'une équation.**

Bar-le-Duc. — Imprimerie Comte-Jacquet





